

# CAN TECHNOLOGY PROTECT AMERICANS FROM INTERNATIONAL CYBERCRIMINALS?

---

## JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT &  
SUBCOMMITTEE RESEARCH AND TECHNOLOGY  
COMMITTEE ON SCIENCE, SPACE, AND  
TECHNOLOGY

HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

MARCH 6, 2014

**Serial No. 113-67**

Printed for the use of the Committee on Science, Space, and Technology



Available via the World Wide Web: <http://science.house.gov>

U.S. GOVERNMENT PRINTING OFFICE

88-137PDF

WASHINGTON : 2014

For sale by the Superintendent of Documents, U.S. Government Printing Office  
Internet: [bookstore.gpo.gov](http://bookstore.gpo.gov) Phone: toll free (866) 512-1800; DC area (202) 512-1800  
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

## COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. LAMAR S. SMITH, Texas, *Chair*

DANA ROHRABACHER, California	EDDIE BERNICE JOHNSON, Texas
RALPH M. HALL, Texas	ZOE LOFGREN, California
F. JAMES SENSENBRENNER, JR., Wisconsin	DANIEL LIPINSKI, Illinois
FRANK D. LUCAS, Oklahoma	DONNA F. EDWARDS, Maryland
RANDY NEUGEBAUER, Texas	FREDERICA S. WILSON, Florida
MICHAEL T. McCAUL, Texas	SUZANNE BONAMICI, Oregon
PAUL C. BROUN, Georgia	ERIC SWALWELL, California
STEVEN M. PALAZZO, Mississippi	DAN MAFFEI, New York
MO BROOKS, Alabama	ALAN GRAYSON, Florida
RANDY HULTGREN, Illinois	JOSEPH KENNEDY III, Massachusetts
LARRY BUCSHON, Indiana	SCOTT PETERS, California
STEVE STOCKMAN, Texas	DEREK KILMER, Washington
BILL POSEY, Florida	AMI BERA, California
CYNTHIA LUMMIS, Wyoming	ELIZABETH ESTY, Connecticut
DAVID SCHWEIKERT, Arizona	MARC VEASEY, Texas
THOMAS MASSIE, Kentucky	JULIA BROWNLEY, California
KEVIN CRAMER, North Dakota	MARK TAKANO, California
JIM BRIDENSTINE, Oklahoma	ROBIN KELLY, Illinois
RANDY WEBER, Texas	
CHRIS COLLINS, New York	
VACANCY	

---

## SUBCOMMITTEE ON OVERSIGHT

HON. PAUL C. BROUN, Georgia, *Chair*

F. JAMES SENSENBRENNER, JR., Wisconsin	DAN MAFFEI, New York
BILL POSEY, Florida	ERIC SWALWELL, California
KEVIN CRAMER, North Dakota	SCOTT PETERS, California
LAMAR S. SMITH, Texas	EDDIE BERNICE JOHNSON, Texas

---

## SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

HON. LARRY BUCSHON, Indiana, *Chair*

STEVEN M. PALAZZO, Mississippi	DANIEL LIPINSKI, Illinois
MO BROOKS, Alabama	FREDERICA WILSON, Florida
RANDY HULTGREN, Illinois	ZOE LOFGREN, California
STEVE STOCKMAN, Texas	SCOTT PETERS, California
CYNTHIA LUMMIS, Wyoming	AMI BERA, California
DAVID SCHWEIKERT, Arizona	DEREK KILMER, Washington
THOMAS MASSIE, Kentucky	ELIZABETH ESTY, Connecticut
JIM BRIDENSTINE, Oklahoma	ROBIN KELLY, Illinois
CHRIS COLLINS, New York	EDDIE BERNICE JOHNSON, Texas
LAMAR S. SMITH, Texas	

# CONTENTS

March 6, 2014

Witness List .....	Page 2
Hearing Charter .....	3

## Opening Statements

Statement by Representative Paul C. Broun, Chairman, Subcommittee on Oversight, Committee on Science, Space, and Technology, U.S. House of Representatives .....	9
Written Statement .....	9
Statement by Representative Dan Maffei, Ranking Minority Member, Subcommittee on Oversight, Committee on Science, Space, and Technology, U.S. House of Representatives .....	10
Written Statement .....	10
Statement by Representative Larry Bucshon, Chairman, Subcommittee on Research and Technology, Committee on Science, Space, and Technology, U.S. House of Representatives .....	11
Written Statement .....	11
Statement by Representative Daniel Lipinski, Ranking Minority Member, Subcommittee on Research and Technology, Committee on Science, Space, and Technology, U.S. House of Representatives .....	12
Written Statement .....	12
Written statement by Representative Eddie Bernice Johnson, Ranking Member, Committee on Science, Space, and Technology, U.S. House of Representatives .....	13

## Witnesses:

Dr. Charles H. Romine, Director, Information Technology Laboratory, National Institute of Standards and Technology .....	14
Oral Statement .....	14
Written Statement .....	17
Mr. Bob Russo, General Manager, Payment Card Industry Security Standards Council, LLC .....	26
Oral Statement .....	26
Written Statement .....	28
Mr. Randy Vanderhoof, Executive Director, Smart Card Alliance .....	35
Oral Statement .....	35
Written Statement .....	37
Mr. Justin Brookman, Director, Consumer Privacy, Center for Democracy & Technology .....	51
Oral Statement .....	51
Written Statement .....	54
Mr. Steven Chabinsky, Senior Vice President of Legal Affairs, CrowdStrike, Inc.; Former Deputy Assistant Director, Federal Bureau of Investigation – Cyber Division .....	65
Oral Statement .....	65
Written Statement .....	67
Discussion .....	75

# IV

## Appendix I: Answers to Post-Hearing Questions

	Page
Dr. Charles H. Romine, Director, Information Technology Laboratory, National Institute of Standards and Technology .....	86
Mr. Bob Russo, General Manager, Payment Card Industry Security Standards Council, LLC .....	91
Mr. Randy Vanderhoof, Executive Director, Smart Card Alliance .....	97
Mr. Justin Brookman, Director, Consumer Privacy, Center for Democracy & Technology .....	107
Mr. Steven Chabinsky, Senior Vice President of Legal Affairs, CrowdStrike, Inc.; Former Deputy Assistant Director, Federal Bureau of Investigation – Cyber Division .....	112

## **CAN TECHNOLOGY PROTECT AMERICANS FROM INTERNATIONAL CYBERCRIMINALS?**

---

**THURSDAY, MARCH 6, 2014**

HOUSE OF REPRESENTATIVES,  
SUBCOMMITTEES ON OVERSIGHT &  
RESEARCH AND TECHNOLOGY  
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,  
*Washington, D.C.*

The Subcommittees met, pursuant to call, at 9:36 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Paul Broun [Chairman of the Subcommittee on Oversight] presiding.

LAMAR S. SMITH, Texas  
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas  
RANKING MEMBER

**Congress of the United States**  
**House of Representatives**

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6371  
[www.science.house.gov](http://www.science.house.gov)

***Can Technology Protect Americans from International  
Cybercriminals?***

Thursday, March 6, 2014  
9:30 a.m. to 11:30 a.m.  
2318 Rayburn House Office Building

Witnesses

**Dr. Charles H. Romine**, Director, Information Technology Laboratory, National  
Institute of Standards and Technology

**Mr. Bob Russo**, General Manager, Payment Card Industry Security Standards  
Council, LLC

**Mr. Randy Vanderhoof**, Executive Director, Smart Card Alliance

**Mr. Justin Brookman**, Director, Consumer Privacy, Center for Democracy &  
Technology

**Mr. Steven Chabinsky**, Senior Vice President of Legal Affairs, CrowdStrike, Inc.;  
Former Deputy Assistant Director, Federal Bureau of Investigation – Cyber  
Division

U.S. House of Representatives  
Committee on Science, Space, and Technology  
Subcommittee on Oversight  
Subcommittee on Research & Technology

**HEARING CHARTER**

*Can Technology Protect Americans from International Cybercriminals?*

Thursday, March 6, 2014  
9:30 a.m. – 11:30 a.m.  
2318 Rayburn House Office Building

**Purpose**

On March 4, 2014, the Subcommittees on Oversight and Research & Technology will hold a joint hearing titled, *Can Technology Protect Americans from International Cybercriminals?*

In light of the recent cyber-crimes against the University of Maryland database and the retail store Target and others over the past holiday season, this hearing will examine the current state of technology and standards to protect Americans from international cybercriminals. The hearing will also address the evolution of cyber-attacks against the U.S. industry from rogue hackers to sophisticated international crime syndicates and foreign governments, including the origination point of many of these crimes.

**Witnesses**

- **Dr. Charles H. Romine**, Director, Information Technology Laboratory, National Institute of Standards and Technology
- **Mr. Bob Russo**, General Manager, Payment Card Industry Security Standards Council, LLC
- **Mr. Randy Vanderhoof**, Executive Director, Smart Card Alliance
- **Mr. Justin Brookman**, Director, Consumer Privacy, Center for Democracy & Technology
- **Mr. Steven Chabinsky**, Senior Vice President of Legal Affairs, CrowdStrike, Inc.; Former Deputy Assistant Director, Federal Bureau of Investigation – Cyber Division

**Background**

The recent cyber-crimes perpetrated against retailers Target, Neiman Marcus, Easton-Bell Sports, Michaels and others, appear to be cases of ‘RAM scraper,’ which is a type of memory-scanning malicious software that enables cybercriminals to grab “unencrypted data during the split-second when it’s vulnerable: while it’s being processed at the register.”<sup>1</sup> In the

<sup>1</sup> John Zorabedian, “Target, Neiman Marcus Card Data Thefts, RAM Scraper Malware, and You,” Sophos Blog, January 24, 2014, available at: <http://blogs.sophos.com/2014/01/24/target-neiman-marcus-card-data-thefts-ram-scraper-malware-and-you/>; hereinafter Sophos Blog.

Target breach, the malware appears to have been “loaded into point-of-sale (POS) terminals, where the unencrypted credit card numbers were skimmed.”<sup>2</sup> Under current Payment Card Industry-Data Security Standard (PCI-DSS) rules:

*“[A]ll payment information must be encrypted when it is stored on the PoS system as well as when it is being transferred to back-end systems. While attackers can still steal the data from the hard drive, they can't do anything with it if it is encrypted, and the fact that the data is encrypted while traveling over the network means attackers can't sniff the traffic to steal anything.*

*This means there is only a small window of opportunity—the instant when the PoS software is processing the information—for attackers to grab the data. The software has to temporarily decrypt the data in order to see the transaction information, and the malware seizes that moment to copy the information from memory.”<sup>3</sup>*

After that, the data is “whisked off to be sorted into bundles and put up for sale on the black market, and printed onto phony cards used by crooks to buy goods at stores.”<sup>4</sup>

In January, the FBI distributed a “confidential, three-page report to retail companies”<sup>5</sup> describing risks posed by RAM scraper malware that infects POS systems, including “cash registers and credit-card swiping machines found in store checkout aisles.”<sup>6</sup> In this memo, the FBI said it has uncovered around twenty cases of cyber-attacks against retailers in the past year that utilized similar methods to those uncovered in the Target incident – with more expected in the near term.<sup>7</sup>

The “accessibility of the malware on underground forums, the affordability of the software, and the huge potential profits to be made from retail POS systems in the United States make this type of financially motivated cybercrime attractive to a wide range of actors.”<sup>8</sup>

These recent cyber-crimes against retailers raise concerns about whether and how Payment Card Industry-Data Security Standards were followed, or if these standards are adequate to ward off such cyber-attacks. If the voluntary standards are not sufficient, how might new technologies and processes defend against such cyber-attacks?

<sup>2</sup> Ibid.

<sup>3</sup> Fahmida Rashid, “How RAM Scraper Malware Stole Data From Target, Neiman Marcus,” SecurityWatch, January 14, 2014, available at: <http://securitywatch.pcmag.com/business-financial/319767-how-ram-scraper-malware-stole-data-from-target-neiman-marcus>.

<sup>4</sup> Sophos Blog, *supra*, note 1.

<sup>5</sup> Jim Finkle and Mark Hosenball, “Exclusive: FBI Warns Retailers to Expect More Credit Card Breaches,” Reuters, January 23, 2014, available at: <http://www.reuters.com/article/2014/01/23/us-target-databreach-fbi-idUSBREA0M1UF20140123>.

<sup>6</sup> Ibid.

<sup>7</sup> Ibid.

<sup>8</sup> Ibid.

## **Technology**

### *Chip and PIN or EMV (Europay, MasterCard and Visa) Cards*

EMV cards contain a computer chip which is a microprocessor embedded in the card that is tamper- and copy-resistant and provides stronger security and protection against fraud by generating a different cryptographic authentication every time it is used. These cards, therefore, are also referred to as “chip cards” or “smart cards.”

The payments industry and retailers have been working together toward a goal of updating credit and debit card security by October 2015. After that date, there will be a liability shift for whoever is utilizing the least secure technology for consumers. In other words:

*“[I]f a merchant is still using the old system, they can still run a transaction with a swipe and a signature. But they will be liable for any fraudulent transactions if the customer has a chip card. And the same goes the other way – if the merchant has a new terminal, but the bank hasn’t issued a chip and PIN card to the customer, the bank would be liable.”<sup>9</sup>*

While EMV or chip and PIN cards are not the silver bullet to prevent all cyber-crimes, this technology has been shown to prevent many such crimes.

## **Key Participants and Considerations**

### *National Institute of Standards and Technology (NIST)*

NIST develops guidelines, standards and technology to help protect domestic IT systems and infrastructure from cyber-attacks and threats to the confidentiality, integrity, and availability of their information and services through initiatives such as the Framework for Improving Critical Infrastructure Cybersecurity, National Strategy for Trusted Identities in Cyberspace (NSTIC), and the National Vulnerability Database (NVD). NIST’s work supports smart card development and applications in the federal and private sectors as well as standards established by the payment card industry for the private sector.

### *Payment Card Industry Security Standards Council (PCI SSC)*

Created in 2006, the PCI SSC is a global open body responsible for the “development, management, education, and awareness of the PCI Security Standards,”<sup>10</sup> and for maintaining and promoting the Payment Card Industry security standards. The Council was created by the five major payment card brands: Visa, MasterCard, American Express, Discover and JCB International.

<sup>9</sup> Tom Gara, “October 2015: The End of the Swipe-and-Sign Credit Card,” The Wall Street Journal, February 6, 2014, available at: <http://blogs.wsj.com/corporate-intelligence/2014/02/06/october-2015-the-end-of-the-swipe-and-sign-credit-card/>.

<sup>10</sup> PCI Security Standards Council, available at: [https://www.pcisecuritystandards.org/organization\\_info/index.php](https://www.pcisecuritystandards.org/organization_info/index.php).

Vulnerabilities in merchants' card-processing systems can appear anywhere including "point of sale devices; personal computers or servers; wireless hotspots or Web shopping applications; in paper-based storage systems; and unsecured transmissions of cardholder data to service providers."<sup>11</sup> The PCI Data Security Standard (DSS) applies to "all entities that store, process, and/or transmit cardholder data. It covers technical and operational system components included in or connected to cardholder data. If you are a merchant who accepts or processes payment cards, you must comply with PCI DSS."<sup>12</sup> However, the Council does not enforce penalties for non-compliance; that is left to each individual payment card brand.

#### *Smart Card Alliance*

Established in 2001, the Smart Card Alliance is a "multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. The Alliance invests heavily in education on the appropriate uses of technology for identification, payment and other applications and strongly advocates the use of smart card technology in a way that protects privacy and enhances data security and integrity."<sup>13</sup>

The Alliance is made up of over 200 members from around the world, including "participants from financial, government, enterprise, transportation, mobile telecommunications, healthcare, and retail industries."<sup>14</sup> Through a combination of educational, industry and member-driven efforts, the Alliance focuses on providing the public with information about smart cards, how they work, and the future of this technology.

#### *Center for Democracy & Technology (CDT)*

CDT's mission is "to conceptualize and implement public policies that will keep the Internet open, innovative, and free."<sup>15</sup> Principles of the Center include:

- **Preserving the Unique Nature of the Internet:** The open, decentralized, and user-controlled nature of the Internet creates unprecedented opportunities for innovation, democratic participation and human development.
- **Enhancing Freedom of Expression:** CDT fights for the right of individuals to communicate, publish and access an unprecedented array of information on the Internet. We oppose governmental censorship and other threats to the free flow of information. We believe that technology tools—not government controls—are the best way to allow families and individuals to make choices about the information they receive on the Internet.
- **Protecting Privacy:** Maintaining privacy on the Internet requires a mix of laws, corporate policies and technology tools giving people control of their personal information.

<sup>11</sup> PCI DSS Quick Reference Guide – Understanding the Payment Card Industry Data Security Standard, Version 2.0 (October 2010).

<sup>12</sup> Ibid.

<sup>13</sup> Smart Card Alliance, available at: <http://www.smartcardalliance.org/pages/alliance>.

<sup>14</sup> Ibid.

<sup>15</sup> Center for Democracy & Technology, available at: <https://www.cdt.org/about>.

- **Limiting Government Surveillance:** CDT advocates for stronger legal standards controlling government surveillance, to keep pace with the growing exposure of personal information as digital media have become central to our lives.<sup>16</sup>

#### *International Crime Syndicates*

The Target retailer hack has been traced back to a “17-year-old hacker from St. Petersburg named Sergey Tarasov. He allegedly wrote the program and then sold it for \$2,000 on a Russian website. At least 40 different criminals, most from the former Soviet Union, used this software to attack American retailers.”<sup>17</sup>

Russia and Russian-speaking countries have typically been responsible for increasingly sophisticated cyber-attacks around the world. With an estimated “annual turnover of more than \$2 billion a year, the Russian cybercrime industry is the source of at least a third of all viruses, Trojans, and other malicious software, or malware, sent around the world.” There are many reasons why Russia “is the leading producer of malicious software,”<sup>18</sup> including inadequate salaries for computer engineers and an unlimited supply of “organized crime with strong ties to the government, which tends to look the other way when it comes to cybercrime.”<sup>19</sup> Most Russian hackers are not prosecuted if they focus their crimes against other countries.

Two years ago, former FBI Director Robert Mueller made the following comment at the annual RSA cyber security conference, “Terrorism does remain the FBI’s top priority, but in the not too-distant-future we anticipate that the cyberthreat will pose the greatest threat to our country.”<sup>20</sup>

#### **Related Legislation**

On March 14, 2013, the Committee passed H.R. 756, the Cybersecurity Enhancement Act and H.R. 967, the Advancing America’s Networking and Information Technology Research and Development Act by voice votes. On April 16<sup>th</sup>, the House overwhelmingly and in a bipartisan manner passed both bills. However, since then, the Senate has taken no action on these bills.

#### *H.R. 756 the Cybersecurity Enhancement Act*

H.R. 756 coordinates research and development activities to better address evolving cyber threats. The legislation promotes much-needed research and development to help create

<sup>16</sup> Ibid.

<sup>17</sup> Ben Plessner, “Skilled, Cheap Russian Hackers Power American Cybercrime,” NBC News, February 5, 2014, available at: <http://www.nbcnews.com/news/world/skilled-cheap-russian-hackers-power-american-cybercrime-n22371>. Feb 5, 2014

<sup>18</sup> Ibid.

<sup>19</sup> Ibid.

<sup>20</sup> Stacy Cowley, “FBI Director: Cybercrime Will Eclipse Terrorism,” CNNMoney, March 2, 2012, available at: [http://money.cnn.com/2012/03/02/technology/fbi\\_cybersecurity/](http://money.cnn.com/2012/03/02/technology/fbi_cybersecurity/).

new technologies and standards that better protect America's information technology systems. To improve America's cybersecurity abilities, this bill strengthens activities in four areas:

- 1) Strategic planning for cybersecurity research and development needs across the federal government;
- 2) Basic research at NSF, which we know is important to increasing security over the long-term;
- 3) NSF scholarships to improve the quality of the cybersecurity workforce; and
- 4) Improved research, development and public outreach organized by NIST related to cybersecurity.

*H.R. 967, the Advancing America's Networking and Information Technology Research and Development Act*

H.R. 967 provides the coordinated R&D efforts necessary to improve cyber and data security nationwide. The bill convenes an interagency working group to identify cloud computing research gaps and examine the potential for using the cloud for federally funded research. The bill also formally codifies and stresses the role of the National Coordination Office (NCO) and implements several recommendations from the President's Council of Advisors on Science and Technology (PCAST) 2007 and 2010 assessments, including:

- 1) Improving program planning and coordination through strategic planning and an Advisory Council with appropriate policy and technical expertise;
- 2) Rebalancing portfolios to focus less on short-term goals and more on large-scale, long-term, interdisciplinary research with the potential to make significant contributions to society and U.S. competitiveness;
- 3) Codifying the National Coordination Office's (NCO) creation of a workshop to explore mechanisms for carrying out collaborative research and development activities for cyber-physical systems with participants from universities, industry, and federal laboratories.

#### Key Questions

- What is the relationship between the federal government and the private sector on issues related to cybersecurity?
- How can the federal government best help and support the private sector to protect its sensitive data?
- How will a transition to EMV chip cards likely impact cyber-attacks against U.S. industries?
- How have the nature and origin of cyber-attacks against the U.S. industry evolved over the past couple of decades?
- Do federal law enforcement agencies have the technology resources and tools they need in their pursuit of international cybercriminals?
- Can new technologies better protect Americans from international cybercriminals?

Chairman BROWN. Good morning, everyone. This joint hearing of the Subcommittee on Oversight and the Subcommittee on Research and Technology will come to order.

Again, good morning and welcome to today's joint hearing. In front of you are packets containing the written testimony, biographies, and truth-in-testimony disclosures for today's witnesses.

Before we get started, since this is a joint hearing involving two Subcommittees, I want to explain how we will all operate procedurally so all Members understand how the question-and-answer period will be handled. We will recognize those Members present at the gavel in order of seniority on the full Committee, and those coming in after the gavel will be recognized in order of arrival.

Now, for the sake of time, in lieu of giving my statement, I will enter it into the record at this point.

[The prepared statement of Mr. Brown follows:]

PREPARED STATEMENT OF SUBCOMMITTEE ON OVERSIGHT CHAIRMAN PAUL BROWN

Good morning. Let me begin by extending a warm welcome to our witnesses and thank you all for appearing. I especially appreciate everyone's patience and flexibility—witnesses and Members alike—in making themselves available today given the weather interruption earlier this week.

Today's hearing is titled "Can Technology Protect Americans from International Cybercriminals?" I hope you can all help us more fully answer that question and explore what specifically is being done to secure U.S. IT infrastructure.

On the one hand, we are here this morning to review what appears to be a rash of recent attacks and successful breaches of American IT infrastructure and computer networks: Target; Neiman Marcus; Easton Sports; Michaels Stores; the University of Maryland; Blue Cross Blue Shield in New Jersey; and now maybe even Sears! A reported 823 million exposed records made 2013 a record year for data breaches. The majority of these data breaches hit businesses and health-care, followed by government, academic, and financial institutions, in that order. In fact, the Identity Theft Center, a non-profit organization that tracks data theft, reported that health-care insurance providers and organizations suffered 267 breaches, or 43 percent of all attacks in 2013. That's significantly higher than the business sector, comprised of retailers, tech companies and others. It seems like an epidemic, and the clear implications of people's privacy being violated concerns me greatly.

On the other hand, fraud and breaches within the retail credit card and debit card industry only amount to five-hundredths of 1% of sales, or five cents on the dollar. And that loss has been declining. In other words, more records are being exposed, but the financial damage may be less. Is this a growing problem justifying more attention and effort, or an example of the ongoing, successful efforts of the private sector, with the help of the government's experience, knowledge, and cooperation to counter these attacks? I take pride in noting that financial technology companies in my home state of Georgia handle over 60 percent of all payment card transactions in America. These Georgia companies are industry leaders in consumer protection and data security, as documented in a February 23rd piece in the Peach Pundit by the CEO of the Electronic Transactions Association.

Today, among other things, we will hear what the private sector is doing in response to the market forces of risk, cost, liability, and reward. I would suggest those free market incentives and disincentives and the right of free association and cooperation are sufficient and the most effective at addressing the evolving, quick-moving threat of sophisticated hacking organizations and cybercriminals. The fact that the payment industry and retailers have been actively working together to make the necessary investments to tighten credit card and debit card security next year by transitioning to "smart or chip card" technology is proof of that.

Nevertheless, the organized, international nature of the new IT threat to intellectual property, trade secrets and other proprietary data, personally identifiable information, medical and insurance records, financial resources, and even top secret material, makes this a critical danger to our economic and national security. We will hear today that China and Russia are actively and aggressively waging economic war on us with massive hacking espionage campaigns. This is very disconcerting, and I look forward to the discussion about the role of law enforcement and intel-

ligence capabilities to deter, detect, and punish global cybercrime syndicates, and whether they need more technological tools and resources.

After all, before former FBI Director Robert Mueller stepped down, he declared that “in the not too-distant-future we anticipate that the cyber threat will pose the greatest threat to our country.” Well, it will be interesting to hear what the former FBI Deputy Assistant Director for Cyber, who served under Director Mueller, has to say in his testimony.

Chairman BROWN. And now, I will recognize my good friend, Mr. Maffei, for his statement.

Mr. MAFFEI. Thank you, Mr. Chairman. And I will follow your lead and also ask unanimous consent to put my opening statement into the record. You have to say so ordered.

Chairman BROWN. Okay. Without objection.

[The prepared statement of Mr. Maffei follows:]

PREPARED STATEMENT OF SUBCOMMITTEE ON OVERSIGHT  
RANKING MINORITY MEMBER DAN MAFFEI

Cybercrime occurs on a daily basis. Widespread breaches, like the recent data breach at Target, affected up to 110 million people by exposing their personal data and credit card information. Smaller breaches can still have serious economic consequences. Last year, hackers with reported links to Al Qaeda engaged in hacking the phone systems of small businesses in New York, including in my district in Syracuse, New York. One of the companies hacked, an Albany-based dry cleaner, halted plans to expand in Syracuse because they were struggling to pay the \$150,000 phone charges they incurred as a result of this attack. This particular breach resulted in more than 75,000 minutes of overseas calls to Zimbabwe, Bosnia, the Congo, Libya and the Maldives.

Last year alone half a billion records of personally identifiable information, including names, emails, credit card numbers and passwords were leaked through data breaches according to an IBM cyber-threat report. But many breaches go unreported. Others go undetected. The full scale and consequence of cybersecurity threats cannot be accurately assessed.

When cybercriminals obtain credit card information on tens of millions of consumers from a retail establishment we all end up paying. Retailers have to pass along the costs for these security incidents through increased prices as a result of fraud, enhanced security upgrades, and potential litigation costs. When foreign governments infiltrate our government agencies, it jeopardizes our national and economic security. When an individual employee at a university, hospital or insurance company steals the digital data of students, patients or clients to engage in identity theft, there are real consequences for Americans.

I do not believe there is a silver bullet to preventing cyber-threats or eliminating the inadvertent disclosure of personal privacy-related data. Technology alone cannot protect us. This is a multifaceted threat and requires a multi-pronged response. A combination of corporate awareness, federal policies, the proper implementation of security standards, employee and consumer training, and due diligence along the chain of information play a critical role in confronting this growing cyber menace.

There are some technical solutions that can certainly help in countering this threat. The migration of so called E-M-V chip cards in the U.S. and the use of “chip and PIN” transactions can play a role. While this will help counter fraudulent person-to-person transactions, they will not stop all fraudulent transactions, like online sales where a card is not present. Online retail sales in the U.S. alone are expected to grow from \$231 billion in 2012 to \$370 billion by 2017, making online financial transactions an even more appealing avenue for cybercriminals.

Standards are another technical solution that can play a key role in helping secure IT systems against a wide-range of cyber-threats. The National Institute of Standards and Technology recently released its “Framework for Improving Critical Infrastructure Cybersecurity.” This guide can help federal agencies and private industry alike implement reliable and robust IT networks that are as safe and secure as possible.

I am concerned however, that industry is not doing enough to protect itself and to protect our data from these various cyber threats. The Payment Card Industry (or PCI) has its own Security Standards Council and we have a witness from the council testifying here today. His testimony clearly says—quote: “the PCI Standards

are the best line of defense against the criminals seeking to steal payment card data.” While the efforts of the industry to police itself are laudable, a recent 2014 report by Verizon called the “PCI Compliance Report” found that only 11.1 percent of the payment card industry companies that it surveyed in 2013 were “fully” compliant with the PCI “Data Security Standard.” This was a decline of nearly 50 percent from the 2010 Verizon “PCI Compliance Report” that showed 22 percent of companies in the Payment Card Industry surveyed in 2009 were “fully” compliant with this standard.

It is unclear why the application of these industry endorsed standards has declined but it is a troubling trend. This is particularly troubling since even the PCI Security Standards Council has said that they have seen a correlation between successful cyber-attacks and the lack of compliance with its standards. We need to figure out a way to either incentivize industry to act or to mandate a requirement that they must act.

It is important that we explore these issues to help understand what the private sector is doing to protect consumer data and how we can be effective partners. But I think it is equally important to understand what the commercial market is doing with consumer data.

We are all sharing more data with more sources all the time. As we share more personal data the opportunities for that data to be stolen, sold or lost escalates. We provide detailed financial data to our banks. Our local grocery store knows the food we eat, the beverages we drink and the toothpaste we use. Facebook knows who we associate with, our favorite movies, books and vacation spots. Google Maps knows where we’ve been and where we’re going. How private industry maintains this data, for how long and how securely is important to every consumer, including me. I hope that Mr. Brookman, a consumer privacy expert from the Center for Democracy & Technology, and one of our witnesses here today, can offer some suggested guidance on how Congress should be thinking about these issues that affect the privacy and security of all of us.

I look forward to hearing from our witnesses and I appreciate the Chairman calling this hearing today. I yield back.

Mr. MAFFEI. And the only thing I will say is I want to thank you, Mr. Chairman, and also Chairman Bucshon and Ranking Member Lipinski for having this hearing. I see the Chairman of the full Committee is here and I want to thank him and my good friend Elizabeth Esty is also here, too.

So this is a very important and substantive issue and I really appreciate you doing this and I think it is a very good issue for our Committee to be looking at.

I yield back.

Chairman BROUN. Thank you, Mr. Maffei. I now recognize Dr. Bucshon for his statement.

Mr. BUCSHON. Chairman, I also ask unanimous consent to submit my statement for the record.

Chairman BROUN. Without objection, so ordered.

[The prepared statement of Mr. Bucshon follows:]

PREPARED STATEMENT OF SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY  
CHAIRMAN LARRY BUCSHON

I would like to welcome everyone to today’s hearing on the role of technology in protecting Americans from cybercriminals.

As Dr. Broun stated, many Americans have experienced security breaches in the past few years. Universities, small grocery stores and retailers in Indiana have all experienced security breaches recently. Along with the national retailer security breaches, we have heard about recently in the news, these smaller instances show how all individuals and consumers are threatened by this growing problem.

According to a poll conducted by Defense News, leaders in national security policy, the military, congressional staff, and the defense industry believe cybersecurity is the top threat to our national security.

While there is no question the federal government plays a role in preventing these security breaches, we must ensure we are using our resources as efficiently and effectively as possible.

The Science, Space and Technology Committee was responsible for two pieces of relevant legislation that passed the House last year.

H.R. 756, the Cybersecurity Enhancement Act, strengthens coordination and provides for strategic planning of cybersecurity research and development between government agencies. While the federal effort to prevent cyber attacks from happening is commendable, we must ensure that these well-intentioned programs are not duplicative or inefficient.

Another piece of legislation that the House passed last year is H.R. 967, the Advancing America's Networking and Information Technology Research and Development Act, which also provides for coordination of the federal investment in research and development of unclassified networking, computing and cybersecurity technology.

These two Science Committee bills both passed the House overwhelmingly with bipartisan support but have been stalled in the Senate, which has not yet indicated if they will act on these vital bills or not. It is my hope that we will see the Senate move these bills forward soon with the active help and support of the cybersecurity community and its stakeholders.

I want to thank the witnesses for participating in today's hearing and look forward to their testimony on private sector initiatives and how we can help leverage these efforts.

Chairman BROWN. Mr. Lipinski, you are recognized for your statement.

Mr. LIPINSKI. You mean I don't get everyone's five minutes for 20 minutes total?

No, thank you, Mr. Chairman. Thank you for holding this hearing. It is very important issue as we keep seeing unfortunately more cyber attacks and hacking, other ways of stealing people's personal information, so I thank you for holding this hearing.

I ask unanimous consent to submit my opening statement for the record.

Chairman BROWN. Without objection, so ordered.

[The prepared statement of Mr. Lipinski follows:]

PREPARED STATEMENT OF SUBCOMMITTEE ON RESEARCH & TECHNOLOGY  
RANKING MINORITY MEMBER DAN LIPINSKI

Thank you Mr. Chairman. And thank you to our witnesses for being here today after some rescheduling earlier in the week.

I've spoken in this Committee many times about the threats posed by cybercrime, and each time there have been recent and potentially more serious attacks to illustrate the point. This time, data breaches at Target and Neiman Marcus collectively resulted in over 100 million records being stolen in the form of personal and credit card information. In total, payment card fraud was responsible for over 11 billion dollars in losses in 2012, with around half of that amount coming from the US. And this figure doesn't account for many other losses associated with identity theft.

Simply put, cybercrime threatens businesses of all sizes and every single American. As such, reducing our risk and improving the security of cyberspace will take the collective effort of both the Federal Government and the private sector, as well as scientists, engineers, and the general public.

Research efforts by the Federal Government and standards developed in conjunction with the private sector will play a big part in addressing cybercrime. The NSF and NIST have lead roles in these respective tasks. I'm interested in hearing more from Dr. Romine about NIST's recent efforts in these areas including the cybersecurity framework for critical infrastructure released last month.

However, it's worth pointing out that it doesn't matter how good our technology is or how current our standards are if people don't use the technology correctly or adopt the standards. You can have the most up-to-date server in the world, but if someone doesn't change the default password or chooses an easily guessed password, no system will be safe. Consider that a Verizon report found that last year only 11% of companies surveyed were fully compliant with PCI standards. In many

ways, people are the weakest link in this process, and understanding how people make decisions—and encouraging better decisions—through social science research must be a part of our efforts to mitigate risk.

To help address some of our nation's cyber threats, Congressman McCaul and I have introduced the Cybersecurity Enhancement Act during the last three congresses. The bill would improve cybersecurity by building strong public-private partnerships, improving the transfer of cybersecurity technologies to the marketplace, training a cybersecurity workforce for both the public and private sectors, and coordinating and prioritizing federal cybersecurity R&D efforts. We passed the bill in the House last year but are still awaiting action in the Senate. Hopefully with increased focus on cybersecurity issues we can finally break through the logjam and get the Senate to act on a bipartisan bill that will address our most immediate research and workforce needs.

Once again, thank you Mr. Chairman for holding this hearing. I look forward to hearing from our witnesses. And with that, I yield back.

Chairman BROWN. Now, I recognize the Chairman of the full Committee for his statement if he so desires. Mr. Smith.

Chairman SMITH. Thank you, Mr. Chairman. I will ask my opening statement be made a part of the record as well.

Chairman BROWN. Without objection, so ordered.

Chairman BROWN. Now, if there are any other Members who wish to submit an opening statement, your statements will be added to the record at this point.

[The prepared statement of Ms. Johnson follows:]

PREPARED STATEMENT OF FULL COMMITTEE RANKING MEMBER EDDIE BERNICE JOHNSON

Thank you, Mr. Chairman. This morning we are examining how technology can help protect Americans against cyber-attacks.

Unfortunately, we have seen a string of cyber-attacks recently. Last year, Target suffered a massive data breach resulting in the loss of millions of debit and credit card numbers. Neiman Marcus, a store based in my home state of Texas, experienced a data breach that involved over a million credit and debit cards last year as well. These breaches exposed the financial and personal information of millions of Americans.

Data breaches are devastating. They cause Americans to lose trust in private and public institutions and result in significant economic losses. Data breaches can also result in intellectual property losses, which can include a company's research and development, leading to millions and billions of dollars in lost profits. The Ponemon Institute estimates that the cost of data breaches due to fines, loss of intellectual property, customer trust and capital equal \$136 per lost record. This translates into \$68 billion in losses globally last year alone.

This morning we will hear about computer chip-based credit cards, known as the "chip-and-pin" cards. Although it seems like these "chip-and-pin" cards would help reduce counterfeiting of stolen credit cards, it is not clear that they would have prevented the recent attacks on Target and Neiman Marcus. To help prevent further similar cyber-attacks, we will need other technologies.

But new technologies alone will not prevent cyber-attacks. New technologies will need to be paired with training and education efforts. Email attachments carrying malware are the most common way attackers get into a computer. To stop that from happening, we need training and education about proper computer security for employees and individuals.

There are a number of federal efforts in this area including at the National Institute of Standards and Technology, which has played an important role in cybersecurity efforts for decades. NIST is the agency tasked with developing standards and guidelines for Federal information systems.

Additionally, NIST is the lead agency for the National Initiative for Cybersecurity Education; they developed the National Strategy for Trusted Identities in Cyberspace; they run a National Cybersecurity Center of Excellence; and they maintain a National Vulnerability Database.

We are fortunate to have Dr. Romine here this morning who can tell us more about these and additional cybersecurity efforts at NIST. Last month, NIST released a Framework for Improving Critical Infrastructure Cybersecurity, which provides a

common language for understanding and managing cybersecurity risks. In our discussion of new technologies, we should be discussing how the federal government can incentivize the public sector to adopt cybersecurity best practices and standards that are included in the Framework.

To prevent cyber-attacks will take an all-hands-on-deck approach. I look forward to working with my colleagues on both sides of the aisle on how the federal government can help with the development and adoption of new cybersecurity technologies.

I would like to thank the witnesses for being here today. Thank you, Mr. Chairman. I yield back the balance of my time.

Chairman BROWN. At this time I would like to introduce our panel of witnesses. Our first witness is Dr. Charles Romine, Director of the Information Technology Laboratory at the National Institute of Standards and Technology, NIST. Our second witness is Mr. Bob Russo, General Manager of the Payment Card Industry Security Standards Council. Our third witness is Mr. Randy Vanderhoof, Executive Director of the Smart Card Alliance. And our fourth witness is Mr. Justin Brookman, Director of Consumer Privacy at the Center for Democracy & Technology. Gentlemen, welcome. We are glad to have all of you here today.

Our final witness is Mr. Chabinsky, Senior Vice President of Legal Affairs at CrowdStrike, Incorporated; Former Deputy Assistant Director at the Federal Bureau of Investigation's FBI's Cyber Division. I welcome you, too, sir. I apologize. I was rushing along to get into this hearing because we are going to have votes very shortly.

And so just for everybody's information, we are going to try to get through all of our witnesses' statements as quickly as possible. If you would, try to limit your testimony to five minutes each. You will have a light in front of you. When it turns red, please be through so we can try to hear everybody before we have to run off to vote and then we will come back for questions. We will get as far along as we can.

As the witnesses should know, spoken testimony is limited to five minutes. Then, after that, Members will have five minutes each to ask you all questions. Upon the hearing, we will submit questions for the record, and please expeditiously answer these questions and get them back to the Committee.

Now, it is the practice of this Subcommittee on Oversight to receive testimony under oath. If you would all please stand and raise your right hand unless you have an objection to taking an oath. Does anybody have an objection to taking an oath?

No. Okay. I see them all shake their head side to side indicating no.

Okay. Do you solemnly swear and affirm to tell the whole truth and nothing but the truth, so help you God?

Very good. Please be seated.

Let the record reflect that all the witnesses participating have taken the oath.

Now, I recognize Dr. Romine for five minutes.

**TESTIMONY OF DR. CHARLES H. ROMINE, DIRECTOR,  
INFORMATION TECHNOLOGY LABORATORY,  
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY**

Dr. ROMINE. Thank you. Chairmen Broun and Bucshon, Ranking Members Maffei and Lipinski, and Members of the Subcommittees,

I am Dr. Charles Romine, the Director of the Information Technology Lab at NIST. Thank you for the opportunity to discuss NIST's role in cybersecurity and our perspective on recent cyber thefts.

Cyber thefts can occur at a scale unlike physical crimes. As we know, one breach can affect thousands if not millions of citizens. Cyber thefts are often perpetrated at the speed of electronic transactions, making interception difficult and placing a strong reliance on preventative security controls.

In response to the hearing title "Can Technology Protect Americans from International Cyber Criminals?" my response would be that it takes a holistic approach that includes technology, training and awareness, policy, legal, economic, and international efforts to bring cyber theft and other cyber threats under control.

I will discuss some of NIST's activities that accelerate the development and deployment of security technologies and assist our stakeholders and partners in protecting their information and communications infrastructure against cyber threats.

In the area of cybersecurity, NIST has worked with Federal agencies, industry, and academia since 1972. Our role—to research, develop, and deploy information security standards and technology to protect information systems against threats to the confidentiality, integrity, and availability of information and services—was strengthened through the Computer Security Act of 1987 and reaffirmed through the Federal Information Security Management Act of 2002 known as FISMA.

NIST accomplishes its mission in cybersecurity through collaborative partnerships. The resulting NIST special publications and interagency reports provide operational and technical security guidelines for Federal agencies and cover a broad range of topics such as electronic authentication and malware.

NIST maintains the National Vulnerability Database, or NVD, a repository of standards-based vulnerability management reference data which enables security automation capabilities for all organizations. The payment card industry uses the NVD vulnerability metrics to discern the IT vulnerability in point-of-sale devices and determine acceptable risk.

NIST researchers develop and standardize cryptographic mechanisms used worldwide to protect information. The NIST algorithms and guidelines are developed in a transparent and inclusive process leveraging cryptographic expertise around the world. The results are in standard interoperable cryptographic mechanisms that can be used by all.

The impact of NIST's activities under FISMA extended beyond enabling protection of federal IT systems. They provide the cybersecurity foundations for the public trust that is essential to realizing the national and global economic productivity and innovation potential of electronic business.

Many organizations voluntarily follow NIST's standards and guidelines reflecting their worldwide acceptance. NIST works extensively in smart card standards and guidelines. NIST developed the standard for the U.S. Government personal identity verification card and actively works on global cybersecurity standards for use in smart cards, smart card cryptography, and others.

As you know, NIST spent the last year working to convene the U.S. critical infrastructure sectors to build a cybersecurity framework as part of Executive Order 13636. This cybersecurity framework released last month was created through collaboration between industry and government and consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The framework is already being implemented by industry, adopted by infrastructure sectors, and is reducing cyber risks to our critical infrastructure, including the finance industry.

The 2013 data breach investigations report noted that in 2012 76 percent of network intrusions exploited weak or stolen credentials. Target has revealed that the compromised credential of one of its business partners was the vector used to access its network.

NIST houses the National Program Office at the National Strategy for Trusted Identities in Cyberspace, or NSTIC, which is addressing this most commonly exploited vector of cyber attack, the inadequacy of passwords for authentication. NSTIC is addressing this issue by collaborating with the private sector, including funding 12 pilots, to catalyze a marketplace of better identity and authentication solutions.

Another critical component of NIST's cybersecurity work is the National Cybersecurity Center of Excellence, a partnership between NIST, the State of Maryland, Montgomery County, and the private sector, which is accelerating the adoption of applied, standards-based solutions to cybersecurity challenges. NIST recognizes our essential role in helping counter cyber theft and cyber threats. We look forward to continuing our work along with our federal government partners, private sector collaborators, and international colleagues to improve upon the comprehensive set of technical solutions, standards, guidelines, and best practices necessary to realize this vision.

Thank you for the opportunity to testify today on NIST's work in cybersecurity and to share some of the specific work we do to assist organizations to reduce risks due to cyber theft, and I would be happy to answer any questions.

[The prepared statement of Dr. Romine follows:]

Testimony of

Charles H. Romine  
Director  
Information Technology Laboratory  
National Institute of Standards and Technology  
United States Department of Commerce

Jointly before the  
United States House of Representatives  
Committee on Science

Subcommittee on Oversight  
and  
Subcommittee on Research and Technology

*“Can Technology Protect Americans from International  
Cybercriminals?”*

March 4, 2014

## Introduction

Chairmen Broun and Bucshon, Ranking Members Maffei and Lipinski and Members of the Subcommittees, I am Dr. Charles Romine, the Director of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology (NIST). Thank you for the opportunity to appear before you today to discuss our role in cybersecurity and our perspective on the recent cybercriminal activities.

## Background

Cybertheft can occur at a scale unlike physical crimes. It can have multiple victims and a much larger impact than would be possible in conventional criminal activity. As we know, one breach can affect thousands – if not millions - of citizens. Cybertheft also can be perpetrated at the speed of electronic transactions. This makes interception difficult and places a strong reliance on preventive security controls. They also can occur without the physical presence of the criminal. This is possible because we work and live in an increasingly interconnected digital world. This introduces jurisdiction, legal and policy complexities as well as difficulty in attribution to the criminals themselves.

In response to the title of the hearing: "Can Technology Protect Americans from International Cybercriminals?" – my response would be: technology alone cannot solve these problems. However, we do believe that effective use of technology can make it more difficult for criminals to perpetrate these crimes, can make it easier for organizations to recover from serious incidents, and can, in some cases, prevent such incidents from occurring.

For example, technology can make it difficult to clone payment cards with stolen credentials or use the information to make online purchases. Smart cards using chip-and-pin technologies can make theft of the information stored on the card more difficult; however, often the attacks and exploits are not on the cards themselves, but are instead against the supporting payment infrastructure. We believe it takes a holistic approach that includes technology, training and awareness, policy, legal, economic and international efforts, to bring cybertheft, one of many different cyberthreats we face, under control.

With that background, today I would like to discuss some of NIST's activities that accelerate the development and deployment of security technologies and assist the US Government and other stakeholders and partners in protecting their information and communications infrastructure against cyberthreats, including cybertheft.

## The Role of NIST in Cybersecurity

NIST's overall mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that

enhance economic security and improve our quality of life. Our work in addressing technical challenges related to national priorities has ranged from projects related to the Smart Grid and electronic health records to atomic clocks, advanced nanomaterials, and computer chips.

In the area of cybersecurity, we have worked with federal agencies, industry, and academia since 1972, starting with the development of the Data Encryption Standard, when the potential commercial benefit of this technology became clear. Our role, to research, develop and deploy information security standards and technology to protect information systems against threats to the confidentiality, integrity and availability of information and services, was strengthened through the Computer Security Act of 1987 and reaffirmed through the Federal Information Security Management Act of 2002 (FISMA).

NIST accomplishes its mission in cybersecurity through collaborative partnerships with our customers and stakeholders in industry, government, academia, standards bodies, consortia and international partners.

Our broader work in the areas of information security, trusted networks, and software quality is applicable to a wide variety of users, from small and medium enterprises to large private and public organizations, including federal government agencies and companies involved with critical infrastructure.

We employ collaborative partnerships with our customers and stakeholders to take advantage of their technical and operational insights and to leverage the resources of a global community. These collaborative efforts, and our private sector collaborations in particular, are constantly being expanded by new initiatives, including in recent years through the National Initiative for Cybersecurity Education (NICE), the National Strategy for Trusted Identities in Cyberspace (NSTIC), the National Cybersecurity Center of Excellence (NCCoE), and in implementation of Executive Order 13636, "Improving Critical Infrastructure Cybersecurity."

#### **NIST Cybersecurity Research, Standards and Guidelines**

The E-Government Act recognized the importance of information security to the economic and national security interests of the United States. The Federal Information Security Management Act of 2002 (FISMA), Title III of the E-Government Act, included duties and responsibilities for NIST to develop standards and guidelines for Federal information systems.

The NIST Special Publications and Interagency Reports provide those management, operational, and technical security guidelines for Federal agencies and cover a broad range of topics such as Basic Input/Output System (BIOS) management and measurement, key management and derivation, media sanitization, electronic authentication, security automation, Bluetooth and wireless protocols, incident handling and intrusion detection, malware, cloud computing, public key infrastructure,

risk assessments, supply chain risk management, authentication, access control, security automation and continuous monitoring.

Beyond these documents - which are peer-reviewed throughout industry, government, and academia - NIST conducts workshops, awareness briefings, and outreach to ensure comprehension of standards and guidelines, to share ongoing and planned activities, and to aid in scoping guidelines in a collaborative, open, and transparent manner.

In addition, NIST maintains the National Vulnerability Database (NVD), a repository of standards-based vulnerability management reference data. The NVD makes available information on vulnerabilities, impact measurements, detection techniques, and remediation assistance. It provides reference data that enable government, industry and international security automation capabilities. The NVD also plays a role in the efforts of the Payment Card Industry (PCI) to identify and mitigate vulnerabilities. The PCI uses the NVD vulnerability metrics to discern the IT vulnerability in point-of-sale devices and determine what risks are unacceptable for that industry.

NIST researchers develop and standardize cryptographic mechanisms that are used throughout the world to protect information at rest and in transit. These mechanisms provide security services, such as confidentiality, integrity, authentication, non-repudiation and digital signatures, to protect sensitive information. The NIST algorithms and associated cryptographic guidelines are developed in a transparent and inclusive process, leveraging cryptographic expertise around the world. The results are in standard, interoperable cryptographic mechanisms that can be used by all industries.

NIST has a complementary program, in coordination with the Government of Canada, to certify independent commercial calibration laboratories to test commercially available IT cryptographic modules, to ensure that they have implemented the NIST cryptographic standards and guidelines correctly. These testing laboratories exist around the globe and test hundreds of individual cryptographic modules yearly.

#### **NIST Engagement with Industry**

It is important to note that the impact of NIST's activities under FISMA extend beyond providing the means to protect Federal IT systems. They provide the cybersecurity foundations for the public trust that is essential to our realization of the national and global productivity and innovation potential of electronic business and its attendant economic benefits. Many organizations voluntarily follow NIST standards and guidelines, reflecting their wide acceptance throughout the world.

Beyond NIST's responsibilities under FISMA, under the provisions of the National Technology Transfer and Advancement Act (PL 104-113) and related OMB Circular A-119, NIST is tasked with the key role of encouraging and coordinating federal agency use of voluntary consensus standards and participation in the development of

relevant standards, as well as promoting coordination between the public and private sectors in the development of standards and in conformity assessment activities. NIST works with other agencies, such as the Department of State, to coordinate standards issues and priorities with the private sector through consensus standards organizations such as the American National Standards Institute (ANSI), the International Organization for Standardization (ISO), the Institute of Electrical and Electronic Engineers (IEEE), the Internet Engineering Task Force (IETF), and the International Telecommunications Union (ITU).

Partnership with industry to develop, maintain, and implement voluntary consensus standards related to cybersecurity best ensures the interoperability, security and resiliency of the global infrastructure needed to make us all more secure. It also allows this infrastructure to evolve in a way that embraces both security and innovation – allowing a market to flourish to create new types of secure products for the benefit of all Americans.

NIST works extensively in smart card standards, guidelines and best practices. NIST developed the standard for the US Government Personal Identity Verification (PIV) Card, and actively works with the ANSI and the ISO on global cybersecurity standards for use in smart cards, smart card cryptography and the standards for the international integrated circuit card. [ANSI 504; ISO 7816 and ISO 24727]

NIST also conducts cybersecurity research and development in forward looking technology areas, such as security for federal mobile environments and techniques for measuring and managing security. These efforts focus on improving the trustworthiness of IT components such as claimed identities, data, hardware, and software for networks and devices. Additional research areas include developing approaches to balancing safety, security, reliability in the nation's supply chain; enabling mobile device and application security; securing the nation's cyber-physical systems; enabling continuous security monitoring; providing advanced security measurements and testing; investigating security analytics and big data; developing standards, modeling, and measurements to achieve end-to-end security over heterogeneous, multi-domain networks; and investigating technologies for detection of anomalous behavior and quarantines.

In addition, further development of cybersecurity standards will be needed to improve the security and resiliency of critical U.S. information and communication infrastructure. The availability of cybersecurity standards and associated conformity assessment schemes is essential in these efforts, which NIST supports to help enhance the deployment of sound security solutions and builds trust among those creating and those using the solutions throughout the country.

### **Cybersecurity Framework**

As you know, NIST has spent the last year working to convene the US Critical Infrastructure sectors to build a Cybersecurity Framework as part of Executive Order 13636. The Cybersecurity Framework, released last month, was created through

collaboration between industry and government, and consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk. The Framework is already being implemented by industry, adopted by infrastructure sectors and is reducing cyber risks to our critical infrastructure, including the finance industry.

#### **National Strategy for Trusted Identities in Cyberspace**

NIST also houses the National Program Office established to lead implementation of the National Strategy for Trusted Identities in Cyberspace (NSTIC). NSTIC is an initiative that aims to address one of the most commonly exploited vectors of attack in cyberspace: the inadequacy of passwords for authentication.

The 2013 Data Breach Investigations Report (conducted by Verizon in concert with the U.S. Department of Homeland Security) noted that in 2012, 76% of network intrusions exploited weak or stolen credentials. In line with the results of this report, Target has revealed that the compromised credential of one of its business partners was the vector used to access its network.

NSTIC aims to address this issue by collaborating with the private sector to catalyze a marketplace of better identity and authentication solutions – an “Identity Ecosystem” that raises the level of trust associated with the identities of individuals, organizations, networks, services, and devices online. NIST has funded a dozen pilots and supported work in the privately led Identity Ecosystem Steering Group (IDESG) to craft standards to improve authentication online.

#### **National Cybersecurity Center of Excellence**

In 2012, the National Cybersecurity Center of Excellence (NCCoE) was formed as a partnership between NIST, the State of Maryland, and Montgomery County to accelerate the adoption of security technologies that are based on standards and best practices. The center is a vehicle for NIST to work directly with businesses across various industry sectors on applied solutions to cybersecurity challenges. Today the NCCoE has programs working with the healthcare, financial services, and energy sectors in addition to addressing challenges that cut across sectors including: mobile device security, software asset management, cloud security, and identity management.

NIST and the NCCoE work extensively in standards and guidelines, as well as research and development in hardware roots of trust. Stronger security assurances can be possible by grounding security mechanisms in roots of trust. Roots of trust are highly reliable hardware, firmware, and software components that perform specific, critical security functions. Because roots of trust are inherently trusted, they must be secure by design. As such, many roots of trust are implemented in hardware

so that malware cannot tamper with the functions they provide. Roots of trust provide a firm foundation from which to build security and trust.

In 2013, NIST and the NCCOE worked with government and industry partners on guidelines for hardware-rooted security features in mobile devices. These guidelines focus on device integrity, isolation, and protected storage features that are supported by roots of trust, and we continue our work to protect fundamental system firmware, commonly known as the BIOS. NIST continues working with key members of the computer industry on the use of roots of trust to improve the security of BIOS, computers and systems overall.

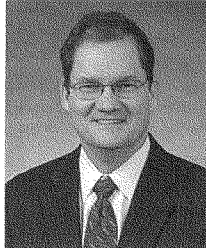
#### **Additional Research Areas**

NIST performs research and development in related technologies, such as the usability of systems including electronic health records, voting machines, biometrics and software interfaces. NIST is performing basic research on the mathematical foundations needed to determine the security of information systems. In the areas of digital forensics, NIST is enabling improvements in forensic analysis through the National Software Reference Library and computer forensics tool testing. Software assurance metrics, tools, and evaluations developed at NIST are being implemented by industry to help strengthen software against hackers. NIST responds to government and market requirements for biometric standards by collaborating with other federal agencies, academia, and industry partners to develop and implement biometrics evaluations, enable usability, and develop standards (fingerprint, face, iris, voice/speaker, and multimodal biometrics). NIST plays a central role in defining and advancing standards, and collaborating with customers and stakeholders to identify and reach consensus on cloud computing standards.

#### **Conclusion**

We at NIST recognize that we have an essential role to play in helping industry, consumers and government entities to counter cybertheft and cyberthreats. We look forward to continuing our work, along with our federal government partners, our private sector collaborators, and our international colleagues to establish and continually improve the comprehensive set of technical solutions, standards, guidelines, and best practices necessary to realize this vision.

Thank you for the opportunity to testify today on NIST's work in cybersecurity, and to share some of the specific work we do to assist organizations in reducing risks due to cybertheft. I would be happy to answer any questions you may have.

**Charles H. Romine**

Charles Romine is Director of the Information Technology Laboratory (ITL). ITL is one of six research Laboratories within the National Institute of Standards and Technology (NIST) with an annual budget of \$120 million, more than 350 employees, and about 160 guest researchers from industry, universities, and foreign laboratories.

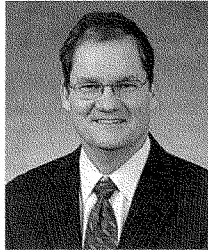
Dr. Romine oversees a research program designed to promote U.S. innovation and industrial competitiveness by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of information systems, including cybersecurity standards and guidelines for Federal agencies and U.S. industry, supporting these and measurement science at NIST through fundamental and applied research in computer science, mathematics, and statistics. Through its efforts, ITL supports NIST's mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Within NIST's traditional role as the overseer of the National Measurement System, ITL is conducting research addressing measurement challenges in information technology as well as issues of information and software quality, integrity, and usability. ITL is also charged with leading the nation in using existing and emerging IT to help meet national priorities, including developing cybersecurity standards, guidelines, and associated methods and techniques, cloud computing, electronic voting, smart grid, homeland security applications, and health information technology.

**Education:**

Ph.D. in Applied Mathematics from the University of Virginia

B.A. in Mathematics from the University of Virginia.

**Charles H. Romine**

Charles Romine is Director of the Information Technology Laboratory (ITL). ITL is one of six research Laboratories within the National Institute of Standards and Technology (NIST) with an annual budget of \$120 million, more than 350 employees, and about 160 guest researchers from industry, universities, and foreign laboratories.

Dr. Romine oversees a research program designed to promote U.S. innovation and industrial competitiveness by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of information systems, including cybersecurity standards and guidelines for Federal agencies and U.S. industry, supporting these and measurement science at NIST through fundamental and applied research in computer science, mathematics, and statistics. Through its efforts, ITL supports NIST's mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Within NIST's traditional role as the overseer of the National Measurement System, ITL is conducting research addressing measurement challenges in information technology as well as issues of information and software quality, integrity, and usability. ITL is also charged with leading the nation in using existing and emerging IT to help meet national priorities, including developing cybersecurity standards, guidelines, and associated methods and techniques, cloud computing, electronic voting, smart grid, homeland security applications, and health information technology

**Education:**

Ph.D. in Applied Mathematics from the University of Virginia

B.A. in Mathematics from the University of Virginia.

Chairman BROWN. Thanks, Dr. Romine.  
Mr. Russo, you are recognized for five minutes.

**TESTIMONY OF MR. BOB RUSSO,  
GENERAL MANAGER, PAYMENT CARD INDUSTRY SECURITY  
STANDARDS COUNCIL, LLC**

Mr. RUSSO. Thank you. My name is Bob Russo and I am the General Manager of the PCI Security Standards Council, a global industry initiative and membership organization focused on securing payment card data. Our approach to an effective security program combines people, process, and technology as key components of protecting payment card data. We believe that development of standards to protect payment card data is something the private sector and specifically PCI is uniquely qualified to do. The global reach, expertise, and flexibility of PCI have made it critical and vital.

Our community of over 1,000 of the world's leading businesses is tackling data security challenges from simple issues—for instance, the word “password” is still the most commonly used password out there—to really complicated issues like proper encryption. Consumers are understandably upset when their payment card data is put at risk, and we know the harm caused by data breaches.

The Council was created to proactively protect consumers' payment card data. Our standards represent a solid foundation for a multilayered security approach. We focus on removing card data if it is no longer needed. Simply put, if you don't need it, don't store it. If you do need it, then protect it. Reduce the incentives for criminals to steal it. Let me tell you how we do that.

The Data Security Standard is built on 12 principles that cover everything from physical security to logical security and much more. This standard is updated regularly through feedback from our global community. In addition, we have developed other standards that cover payment software, point-of-sale devices, the secured manufacturing of cards, and much, much more.

We work on technologies like tokenization and point-to-point encryption to help reduce the amount of card data kept in systems and devalue that information. Tokenization and point-to-point encryption work in concert with other PCI standards to offer additional protections.

Another technology, EMV chip, is an extremely effective method of reducing card fraud in a face-to-face environment. That is why the Council supports its adoption in the United States through organizations such as the EMV Migration Forum. And our standards support EMV today in other worldwide markets.

However, EMV chip is only one piece of the puzzle. Additional controls are needed to protect the integrity of payments online and in other channels. These include encryption, tamper-resistant devices, malware protection, network monitoring, and more. These are all addressed within the PCI standards. Used together, EMV chip and PCI can provide strong protections for payment card data.

But effective security requires much more than just standards. Standards without supporting programs are only tools and not solutions. The Council's training and certification programs have educated tens of thousands of individuals and make it easy for busi-

nesses to choose products that have already been lab-tested and certified as secure.

Finally, we conduct global campaigns to raise awareness of payment card security.

We welcome the Committee's attention to this critical issue. The recent compromises underscore the importance of a multilayered approach to payment card security, and there are clear ways in which the government can help, for example, by leading stronger law enforcement efforts worldwide and by encouraging stiffer penalties for these crimes. Promoting information sharing between public and private sectors also merits attention.

The Council is an active collaborator with government. We work with NIST, with DHS, and many other government entities. We are ready and willing to do much more. The recent breaches underscore the complex nature of payment card security. A multifaceted problem cannot be solved by a single technology, standard, mandate, or regulation. It cannot be solved by a single sector of society. We must work together to protect the financial and privacy interests of consumers.

Today, as this Committee focuses on recent data breaches, we know that the criminals are focusing on inventing the next attacks. There is no time to waste. The PCI Standards Council and business must continue to provide multilayered security protections while Congress leads the efforts to combat global cybercrimes that threaten us all.

We thank the Committee for taking a leadership role in seeking solutions to one of the largest security concerns of our time.

[The prepared statement of Mr. Russo follows:]



**Statement for the Record**

**Bob Russo**  
General Manager  
Payment Card Industry Security Standards Council

Before the Committee on Science, Space, and Technology,  
Subcommittee on Oversight & Subcommittee on Research and Technology  
United States House of Representatives

**Can Technology Protect Americans from International Cybercriminals?**

March 4, 2014  
2318 Rayburn House Office Building

**Introduction**

My name is Bob Russo and I am the General Manager of the Payment Card Industry (PCI) Security Standards Council (SSC), a global industry initiative and membership organization, focused on securing payment card data. Working with a global community of industry players, our organization has created data security standards—notably the PCI Data Security Standard (PCI DSS)—certification programs, training courses, and best practice guidelines to help improve payment card security.

Together with our community of over one thousand of the world's leading businesses, we're tackling data security challenges from password complexity to proper protection of PIN entry devices on terminals. Our work is broad for a simple reason: there is no single answer to securing payment card data. No one technology is a panacea; security requires a multi-layered approach across the payment chain.

The PCI Security Standards Council is an excellent example of effective industry collaboration to develop private sector standards. Simply put, the PCI Standards are the best line of defense against the criminals seeking to steal payment card data. And while several recent high profile breaches have captured the nation's attention, great progress has been made over the past seven years in securing payment card data through a collaborative cross-industry approach, and we continue to build upon the way we protect this data.

Consumers are understandably upset when their payment card data is put at risk of misuse and—while the PCI Security Standards Council is not a name most consumers know—we are sensitive to the impact that breaches cause for consumers. Consumers should take comfort from the fact that a great number of the organizations they do business with have joined the PCI SSC to collaborate in efforts to better protect their payment card data.

### Payment card security: a dynamic environment

Since the threat landscape is constantly evolving, the PCI SSC expects its standards to do the same. Confidence that businesses are protecting payment card data is paramount to a healthy economy and payment process—both in person and online. That's why to date, more than one thousand of the world's leading retailers, airlines, banks, hotels, payment processors, government agencies, universities, and technology companies have joined the PCI Council as members and as part of our assessor community to develop security standards that apply across the spectrum of today's global multi-channel and online businesses.

Our community members are living on the front lines of this challenge and are therefore well placed, through the unique forum of the PCI Security Standards Council, to provide input on threats they are seeing and ideas for how to tackle these threats through the PCI Standards.

The Council develops standards through a defined, published three year lifecycle. Our Participating Organization members told us that three years was the appropriate timeframe to update and deploy security approaches in their organizations. In addition to the formal lifecycle, the Council and the PCI community have the resources to continually monitor and provide updates through standards, published FAQs, Special Interest Group work, and guidance papers on emerging threats and new ways to improve payment security. Examples include updated wireless guidance and security guidelines for merchants wishing to accept mobile payments.

This year, on January 1, 2014, our latest version of the PCI Data Security Standard (PCI DSS) became effective. This is our overarching data security standard, built on 12 principles that cover everything from implementing strong access control, monitoring and testing networks, to having an information security policy. During updates to this standard, we received hundreds of pieces of feedback from our community. This was almost evenly split between feedback from domestic and international organizations, highlighting the global nature of participation in the PCI SSC and the need to provide standards and resources that can be adopted globally to support the international nature of the payment system.

This feedback has enabled us to be directly responsive to challenges that organizations are facing every day in securing cardholder data. For example, in this latest round of PCI DSS revisions, community feedback indicated that changes were needed to secure password recommendations. Password strength remains a challenge—as "password" is still among the most common password used by global businesses—and is highlighted in industry reports as a common failure leading to data compromise. Small merchants in particular often do not change passwords on point of sale (POS) applications and devices. With the help of the PCI community, the Council has updated requirements to make clear that default passwords should never be used, all passwords must be regularly changed and not continually repeated, should never be shared, and must always be of appropriate strength. Beyond promulgating appropriate standards, we have taken steps through training and public outreach to educate the merchant community on the importance of following proper password protocols.

Recognizing the need for a multi-layer approach, in addition to the PCI DSS, the Council and community have developed standards that cover payment applications and point of sale devices. In other areas, based on community feedback, we are working on standards and guidance on other technologies such as tokenization and point-to-point encryption. These technologies can dramatically increase data security at vulnerable points along the transactional chain. Tokenization and point-to-point encryption remove or render payment card information useless to cyber criminals, and work in concert with other PCI Standards to offer additional protection to payment card data.

In addition to developing and updating standards, the PCI community votes annually on which topics they would like to explore with the Council and provide guidance on. Over the last few years the working groups formed by the Council to address these concerns have collaborated with hundreds of organizations to produce resources on third party security assurance, cloud computing, best practices for maintaining compliance, e-

commerce guidelines, virtualization, and wireless security. Other recent Council initiatives have addressed ATM security, PIN security, and mobile payment acceptance security for developers and merchants.

#### **EMV Chip & PCI Standards—a strong combination**

One technology that has garnered a great deal of attention in recent weeks is EMV chip—a technology that has widespread use in Europe and other markets. EMV chip is an extremely effective method of reducing counterfeit and lost/stolen card fraud in a face-to-face payments environment. That is why the PCI Security Standards Council supports the deployment of EMV chip technology.

Global adoption of EMV chip, including broad deployment in the U.S. market, does not preclude the need for a strong data security posture to prevent the loss of cardholder data from intrusions and data breaches. We must continue to strengthen data security protections that are designed to prevent the unauthorized access and exfiltration of cardholder data.

Payment cards are used in variety of remote channels—such as electronic commerce—where today's EMV chip technology is not typically an option for securing payment transactions. Security innovation continues to occur for online payments beyond existing fraud detection and prevention systems. Technologies such as authentication, tokenization, and other frameworks are being developed, including some solutions that may involve EMV chip—yet broad adoption of these solutions is not on the short-term horizon. Consequently, the industry needs to continue to protect cardholder data across all payment channels to minimize the ongoing risks of data loss and resulting cross-channel fraud that may be experienced in the online channel.

Nor does EMV chip negate the need for secure passwords, patching systems, monitoring for intrusions, using firewalls, managing access, developing secure software, educating employees, and having clear processes for the handling of sensitive payment card data. These processes are critical for all businesses—both large retailers and small businesses—who have become a target for cyber criminals. For smaller businesses, EMV chip technology will have a strong positive impact. But if small businesses are not aware of the need to secure other parts of their systems, or if they purchase services and products that are not capable of doing that for them, then they will still be subject to the ongoing exposure of the compromise of cardholder data and resulting financial or reputational risk.

Similarly, protection from malware-based attacks requires more than just EMV chip technology. Reports in the press regarding recent breaches point to the insertion of complex malware. EMV chip technology could not have prevented the unauthorized access, introduction of malware, and subsequent exfiltration of cardholder data. Failure of other security protocols required under Council standards is necessary for malware to be inserted.

Finally, EMV chip technology does not prevent memory scraping, a technique that has been highlighted in press reports of recent breaches. Other safeguards are needed in order to do so. In our latest versions of security standards for Point of Sale devices, (PCI PIN Transaction Security Requirements), the Council includes requirements to further counter this threat. These include improved tamper responsiveness so that devices will "self-destruct" if they are opened or tampered with, and the creation of electronic signatures that prevent applications that have not been "whitelisted" from being installed. Our recently released update to the standard, PTS 4.0, requires a default reset every 24 hours that would remove malware from memory and reduce the risk of data being obtained in this way. By responding to the Council's PTS requirements, POS manufacturers are bringing more secure products to market that reflect a standards development process that incorporates feedback from a broad base of diverse stakeholders.

Used together, EMV chip, PCI Standards, along with many other tools, can provide strong protections for payment card data. I want to take this opportunity to encourage all parties in the payment chain—whether they are EMV chip ready or not—to take a multi-layered approach to protect consumers' payment card data. There are no easy answers and no shortcuts to security.

Global adoption of EMV chip is necessary and important. Indeed, when EMV chip technology does become broadly deployed in the U.S. marketplace and fraud migrates to less secure transaction environments, PCI Standards will remain critical.

#### **Beyond Standards – building a support infrastructure**

An effective security program through PCI is not focused on technology alone; it includes people and process as key parts of payment card data protection. PCI Standards highlight the need for secure software development processes, regularly updated security policies, clear access controls, and security awareness education for employees. Employees have to know not to click on suspicious links, why it is important to have secure passwords, and to question suspicious activity at the point of sale.

Most standards organizations create standards, and no more. PCI Security Standards Council, however, recognizes that standards, without more, are only tools, and not solutions. And this does not address the critical challenges of training people and improving processes.

To help organizations improve payment data security, the Council takes a holistic approach to securing payment card data, and its work encompasses both PCI Standards development and maintenance of programs that support standards implementation across the payment chain. The Council believes that providing a full suite of tools to support implementation is the most effective way to ensure the protection of payment card data. To support successful implementation of PCI Standards, the Council maintains programs that certify and validate certain hardware and software products to support payment security. For example, the Council wants to make it easy for merchants and financial institutions to deploy the latest and most secure terminals and so maintains a public listing on its website for them to consult before purchasing products. We realize it takes time and money to upgrade POS terminals and we encourage businesses that are looking to upgrade for EMV chip to consider other necessary security measures by choosing a POS terminal from this list. Similarly, we are supporting the adoption of point-to-point encryption, and listing appropriate solutions on our website to take a solutions-oriented approach to helping retailers more readily implement security in line with the PCI standards.

Additionally, the Council runs a program that develops and maintains a pool of global assessment personnel to help work with organizations that deploy PCI Standards to assess their performance in using PCI Standards. The Council also focuses on creating education and training opportunities to build expertise in protecting payment card data in different environments and from the various viewpoints of stakeholders in the payment chain. Since our inception, we have trained tens of thousands of individuals, including staff from large merchants, leading technology companies and government agencies. Finally, we devote substantial resources to creating public campaigns to raise awareness of these resources and the issue of protecting payment card data.

The PCI community and large organizations that accept, store, or transmit payment card data worldwide have made important strides in adopting globally consistent security protocols. However, the Council recognizes that small organizations remain vulnerable. Smaller businesses lack IT staff and budgets to devote resources to following or participating in the development of industry standards. But they can take simple steps like updating passwords, firewalls, and ensuring they are configured to accept automatic security updates. Additionally, to help this population, the Council promotes its listings of validated products, and recently launched a program, the Qualified Integrator and Reseller program (QIR), to provide a pool of personnel able to help small businesses ensure high quality and secure installation of their payment systems.

The work of the Council covers the entire payment security environment with the goal of providing or facilitating access to all the tools necessary—standards, products, assessors, educational resources, and training—for

stakeholders to successfully secure payment card data. We do this because we believe that no one technology is a panacea and that effective security requires a multi-layered approach.

#### Public – private collaboration

The Council welcomes this hearing and the government's attention on this critical issue. The recent compromises underscore the importance constant vigilance in the face of threats to payment card data. We are hopeful that this hearing will help raise awareness of the importance of a multi-layered approach to payment card security.

There are very clear ways in which the government can help improve the payment data security environment. For example, by championing stronger law enforcement efforts worldwide, particularly due to the global nature of these threats, and by encouraging stiff penalties for crimes of this kind to act as a deterrent. There is much public discussion about simplifying data breach notification laws and promoting information sharing between public and private sector. These are all opportunities for the government to help tackle this challenge.

The Council is an active participant in government research in this area: we have provided resources, expertise and ideas to NIST, DHS, and other government entities, and we remain ready and willing to do so.

Almost 20 years ago, through its passage of the Technology Transfer and Advancement Act of 1995, Congress recognized that government should rely on the private sector to develop standards rather than to develop them itself. The substantial benefits of the unique, U.S. "bottom up" standards development process have been well recognized. They include the more rapid development and adoption of standards that are more responsive to market needs, representing an enormous savings in time to government and in cost to taxpayers.

The Council believes that the development of standards to protect payment card data is something the private sector, and PCI specifically, is uniquely qualified to do. It is unlikely any government agency could duplicate the expansive reach, expertise, and decisiveness of PCI. High profile events such as the recent breaches are a legitimate area of inquiry for the Congress, but should not serve as a justification to impose new government regulations. Any government standard in this area would likely be significantly less effective in addressing current threats, and less nimble in protecting consumers from future threats, than the constantly evolving PCI Standards.

#### Conclusion

In 2011, the Ponemon Institute, a non-partisan research center dedicated to privacy, data protection, and information security policy wrote, "The Payment Card Industry Data Security Standard (PCI DSS) continues to be one of the most important regulations for all organizations that hold, process or exchange cardholder information."

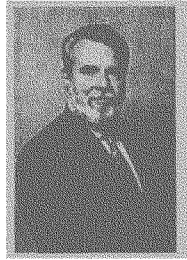
While we are pleased to have earned accolades such as this, we cannot rest on our laurels.

The recent breaches at retailers underscore the complex nature of payment card security. A complex problem cannot be solved by any single technology, standard, mandate, or regulation. It cannot be solved by a single sector of society—business, standards-setting bodies, policymakers, and law enforcement—must work together to protect the financial and privacy interests of consumers. Today, as this committee focuses on recent damaging data breaches, we know that there are criminals focusing on committing or inventing the next threat.

There is no time to waste. The PCI Security Standards Council and business must commit to promoting stronger security protections while Congress leads efforts to combat global cyber-crimes that threaten us all.

We thank the Committee for taking an important leadership role in seeking solutions to one of the largest security concerns of our time.

###

**Bob Russo****General Manager, PCI Security Standards Council**

Bob Russo, the General Manager of the PCI Security Standards Council, works with representatives from American Express, Discover, JCB International, MasterCard, and Visa Inc. to drive awareness and adoption of the PCI Data Security Standard.

Mr. Russo is responsible for driving the organization's growth and development, as well as meeting its goals to create educational programs, establish pools of certified Qualified Security Assessors (QSAs), Internal Security Assessors (ISAs), PCI Forensic Investigators (PFIs), and Approved Scanning Vendors (ASVs), and incorporate feedback from all stakeholders across the payment chain into the work of the Council and the development of new standards. In addition, Mr. Russo oversees the PCI Security Standards Council's training, testing, and certification programs for QSAs, ISAs, PFIs, and ASVs.

Mr. Russo brings more than 35 years of high-tech business management, operations, and security experience to the PCI Security Standards Council. Mr. Russo guides the organization through its crucial charter, focusing on improving data security standards for merchants, banks and other key stakeholders involved in the global payment card transaction process.

Chairman BROWN. Thank you, Mr. Russo.

The buzzer that you hear is for votes on the Floor of the House and so we are going to have to go shortly. We have time for Mr. Vanderhoof to give your testimony for five minutes. And, for Members' information, we will recess right after Mr. Vanderhoof finishes. We will go vote. It is going to be a long series of votes, probably about an hour, maybe a little more. We will come back for Mr. Brookman and Mr. Chabinsky's statement.

And so, Mr. Vanderhoof, you are recognized for five minutes. Please keep it within five minutes. Thank you.

**TESTIMONY OF MR. RANDY VANDERHOOF,  
EXECUTIVE DIRECTOR,  
SMART CARD ALLIANCE**

Mr. VANDERHOOF. Chairman Broun and Chairman Bucshon and Members of the Subcommittee, on behalf of the Smart Card Alliance and its members, I thank you for the opportunity to testify today.

The Smart Card Alliance is a nonprofit organization that provides education about smart card chip technology and applications. In 2012, the Alliance formed the EMV Migration Forum to convene all payments industry stakeholders to advance the migration to EMV in the United States. Collectively, the two organizations have more than 370 member organizations, including American Express, Discover, MasterCard, and Visa and financial institutions, merchants, and other payments industry participants.

My testimony will be about payment security and the increasing threat of cybercrime to steal vulnerable payment data, how EMV chip cards and terminals make payments more secure, and the state of the U.S. migration towards EMV.

As this hearing recognizes, the increasing instances of cybercrime in the United States highlight the need for EMV chip cards. Cybercrime criminals are increasingly targeting retail store chains. The FBI found at least 22 instances of this in the past year. Attacks on retailers are particularly damaging because a single attack can cause millions of dollars' worth of credit card fraud and create the need to close and reissue tens of millions of payment card accounts.

The increase in attempted data breaches on retail systems is due in part to the fact that the U.S. magnetic stripe card data is highly valued by hackers who can sell it on the black market to criminals for large profits. For example, the black market price for several million card accounts believed to be stolen from the Target breach was between \$27 and \$45 each for a period of time. Criminals pay such high prices for U.S. magnetic stripe card data because it is easy to use it to create counterfeit payment cards. This is why the United States is the only region in the world where counterfeit card fraud continues to grow.

It is our best interest to replace magnetic stripe cards with secure EMV chip cards because it will devalue U.S. payments data for criminals. This is mainly because, if stolen, EMV data cannot be used to create usable counterfeit payment cards. And countries that have implemented EMV have seen counterfeit card fraud decline by as much as 67 percent. The positive news is that the U.S.

payment system is already more than two years into a plan to four-year migration to EMV chip technology.

Next, I want to tell you more about EMV chip cards and how they address counterfeit card fraud. EMV is the name of the global standard for chip payment cards and is based on widely used and highly secure smart card technology. Today, 45 percent of the total payment cards in circulation and 76 percent of the POS terminals installed globally are this EMV-enabled device.

EMV prevents counterfeit card fraud in two ways. The first way is the secure storage of the cardholder data inside the chip rather than on the magnetic stripe. Even if the chip data were to be copied, it cannot be used to create another chip card using the same data. Also, EMV transaction data excludes other data needed for magnetic stripe transactions, so it cannot be used to make fraudulent transactions in an EMV or magnetic stripe environment.

The second way is by a one-time unique code called a cryptogram generated by the chip during each payment transaction. The cryptogram proves that the card is authentic and that the transaction data was unique to that card. Therefore, any use of the same unique card data would be detected and the transaction denied.

To put these security benefits into perspective, if EMV chip card data had been present in the retailer systems that were recently victimized, the impact of that data breach would have been significantly lessened for the merchant, the card issuers, and the consumers due to the greatly reduced risk of counterfeiting and resulting card fraud.

The U.S. migration to EMV is complex, expensive, and difficult to coordinate, especially for debit cards. The U.S. payment market, which is larger than all of Europe combined, is the largest individual market to convert to chip cards. This migration has been driven by the payment brands in the form of a fraud liability shift that align around targeted migration dates starting in October 2015. After these dates, the responsibility for fraud resulting from a payment transaction will shift away from the party using the most secure technology. This fraud liability shift is the most effective approach to ensure each party in the payments transaction makes the investment in chip technology.

To date, an estimated 15 to 20 million chip payment cards have been issued to U.S. consumers and retailers have replaced approximately 1 million of the estimated 10 million point-of-sale terminals.

In summary, the predominant use of magnetic stripe payment cards contribute greatly to the U.S. financial markets being targets for cyber thefts and counterfeit card fraud. While a move to EMV chip payments in the United States is a complex and expensive undertaking, it is a critical one that will benefit our entire payment system. I am encouraged by the payments industry and merchants' recognition that we need to move to EMV chip technology quickly and by the fact that chip cards are being used now and retailers are moving to put in place the chip-enabled terminals to begin accepting chip transactions by the industry's target dates.

I thank you for your attention and I welcome any questions from the Committee.

[The prepared statement of Mr. Vanderhoof follows:]

Testimony of Randy Vanderhoof

Executive Director, Smart Card Alliance

Before the Committee on Science, Space and Technology,  
Subcommittees on Oversight and Research & Technology

“Can Technology Protect Americans From International  
Cybercriminals”

March 4, 2014

---

On behalf of the Smart Card Alliance and its members, I thank you for the opportunity to testify today. We applaud the Subcommittees' leadership and foresight in examining important issues in the payments industry, especially on increasing instances of international cybercriminals committing payment data breaches and the role of EMV chip payment technology to help secure the U.S. payments infrastructure.

The Smart Card Alliance is a non-profit organization established in 2001 that provides education about smart card chip technology and applications and operates a collaborative, open forum among leaders in various industries including payments, mobile, transportation, government, healthcare, and access security. The Alliance's members from the payment ecosystem include payment brands, card issuers, payment processors, merchants and technology providers.

Shortly after the four major payments brands, American Express, Discover, MasterCard and Visa, announced incentives to introduce secure EMV chip cards for the U.S. market and aligned timelines for fraud liability shift dates in 2015 and 2017, the Smart Card Alliance organized a new payments-only industry association, the EMV Migration Forum. The Forum was formed specifically to address issues that require broad cooperation and coordination across many constituents in the payments space to ensure the successful adoption of EMV-enabled cards, devices, and terminals across the U.S. market, and to ensure that migration in the U.S. market is efficient, timely and effective. The Forum has more than 150 member companies, including global payments brands, financial institutions, merchants, processors, acquirers, regional debit networks, industry associations and industry suppliers.

The Smart Card Alliance and the EMV Migration Forum have been the leading advocates for accelerating the adoption of secure payments technology to address the growing fraud problem in the United States and to ensure citizens traveling outside of the U.S. will have a safe and convenient payments experience.



191 Clarksville Road  
Princeton Junction, New Jersey 08550 (USA)  
1.800.556.6828  
[www.smartcardalliance.org](http://www.smartcardalliance.org)

The focus of my testimony will be on the state of payment card technology and the payments acceptance ecosystem, including differences between the magnetic stripe cards used in the U.S. and EMV chip cards used in more than 80 countries, the status of U.S. migration to EMV chip cards, and the benefits for the U.S. moving to EMV chip cards to increase security, reduce counterfeit card fraud, and reduce the likelihood of future data breaches by devaluing the payments data that is present in the retail and financial systems.

#### Increasing Instances of Cybercrime in the U.S. Highlight Need for EMV Chip Cards

Cybercrime targeting government and commercial enterprises is a growing problem in the U.S. In 2013, data breaches became more damaging, with one in three people who received a data breach notification letter becoming an identity fraud victim, up from one in four in 2012<sup>1</sup>.

While cybercrime is a known threat across many industries, criminals are increasingly targeting retail store chains with sophisticated attacks in order to extract credit card data from millions of transactions. Attacks against retailers are particularly damaging because of their effects on large numbers of consumers, banks and merchants at the same time. The results of a single attack, which we saw most recently with retailer Target, can be millions of dollars' worth of credit card fraud and the need to close and reissue tens of millions of payment card accounts to prevent further fraud. There are also other unquantified costs of payment data breaches, including the time and money to investigate and clean up after the breach, lost business and damaged reputations for the merchants and banks involved.

The opportunity for huge financial gains with little chance of criminal prosecution from these stolen card accounts also provides the incentive for hackers to penetrate deeper into compromised networks to extract additional personal information beyond payments data, including email addresses and phone numbers, putting consumers' privacy at further risk.

Increasing instances of attacks against retailers are due in part to the fact that U.S. magnetic stripe payment card information is highly valuable data for hackers, who can sell it on the black market to criminals for large profits. For example, the black market price for several million card accounts stolen from the Target breach was between \$26.60 and \$44.80 each prior to Dec. 19, 2013<sup>2</sup>.

Criminals are willing to pay such high prices for U.S. magnetic stripe card data because of the ease with which that data can be used to create counterfeit payment cards for fraud. It's very simple to write stolen magnetic stripe payment card information to a different magnetic stripe payment card. This is why the U.S. is the only region where counterfeit card fraud continues to grow. The U.S. accounted for

<sup>1</sup> Javelin Strategy & Research, "2014 IDENTITY FRAUD REPORT: Card Data Breaches and Inadequate Consumer Password Habits Fuel Disturbing Fraud Trends," February 2014.

<sup>2</sup> Krebs, Brian. "Fire Sale on Cards Stolen in Target Breach." *Krebs on Security*. Web. 26 Feb. 2014.  
<<http://krebsonsecurity.com/2014/02/fire-sale-on-cards-stolen-in-target-breach/>>.



191 Clarksville Road  
Princeton Junction, New Jersey 08550 (USA)  
1.800.556.6828  
[www.smartcardalliance.org](http://www.smartcardalliance.org)

47.3% of global fraud losses in 2012, despite only accounting for 23.5% of the total transactions, and U.S. issuer losses due to counterfeiting account for 26.5% of global fraud losses<sup>3</sup>.

The financial industry has very strict data security standards, called the Payment Card Industry Data Security Standard (PCI DSS), in place to protect payments data and other sensitive personal information captured and stored by retail systems and processors. These standards and best practices are effective deterrents against a lot of criminal activity, but not enough for increasingly sophisticated criminals and attacks. Additional security measures are needed and are already used globally including EMV chip cards, advanced encryption technologies and tokenization.

EMV chip cards in particular can reduce the threat of financial cybercrime by removing the economic incentive for criminals. Replacing magnetic stripe payment data with secure EMV chip payment data devalues U.S. payment data in the eyes of criminals because, if stolen, EMV chip payment data cannot be used to create counterfeit payment cards.

The positive news is that the U.S. payments system is undertaking a migration to EMV chip card technology, and this will present significant barriers for criminals engaging in payment card counterfeiting. Although the U.S. payments system is complex, the industry has recognized the need to move as quickly as possible to EMV chip card payments. I am encouraged by the movement and progress from all industry stakeholders towards implementation of the technology.

Next, I will explain EMV chip card technology and why it is secure, how it can help to address mounting U.S. payment data security problems, and what the current status of U.S. EMV migration is.

#### Introduction to EMV Chip Payment Technology

EMV chip payment cards are based on widely used and highly secure smart card technology, also referred to as “smart chip” technology. Smart cards – which can look like a card but can also take on different forms – have embedded integrated circuit chips, powerful minicomputers that can be programmed for different applications. Through the chip, the smart card can store and access data and applications securely, and exchange data securely with readers and other systems. Smart cards are ideal for many applications, especially payments, because they provide high levels of security and privacy protection, are easily carried, and do not require their own power source to operate effectively.

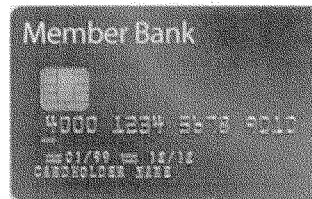


Figure 1: EMV chip card

Smart cards are currently used to secure many applications worldwide, including:

<sup>3</sup> "Global Credit, Debit, and Prepaid Card Fraud Losses Reach \$11.27 Billion in 2012." The Nilson Report, Web. 27 Feb. 2014.



191 Clarksville Road  
Princeton Junction, New Jersey 08550 (USA)  
1.800.556.6828  
[www.smartcardalliance.org](http://www.smartcardalliance.org)

- Identity applications including employee ID badges for physical access to buildings and secure computer and network access; citizen ID documents; electronic passports; driver's licenses; and online authentication devices. Today, smart card technology is used by all U.S. federal employees and contractors with Personal Identity Verification (PIV) credentials to secure access to government systems and buildings; in U.S. citizens' passports to secure identity information; and in federal programs like the TSA First Responder Authentication Credential (FRAC), the TSA Transportation Worker Identification Credential (TWIC) and the Department of Defense Common Access Card (CAC)
- Healthcare applications including citizen health ID cards; health provider ID cards; portable medical records cards. Smart card technology is now being recommended in legislation to create a pilot for a proposed Medicare Common Access Card (H.R. 3024)
- Mobile applications including billions of mobile phone subscriber identity modules (SIMs) in use today, plus in NFC-enabled phones to secure mobile wallets
- And lastly, with global payment standard EMV chip cards, now used in more than 80 countries worldwide with 1.6 billion payments cards issued to date, and the focus of this testimony

#### EMV: A Global Perspective

It was growing counterfeit card fraud that originally led the global payments industry to move to smart chip technology for bank cards and to develop the global EMV standard for bank cards based on chip card technology. The EMV specification, first available in 1996 and managed by EMVCo, defines the global interoperable standard for smart chip-based bank cards.

Financial institutions in Europe, Latin America, Asia/Pacific and Canada are issuing EMV chip cards for credit and debit payment or migrating to EMV issuance. According to EMVCo, approximately 1.6 billion EMV cards have been issued globally and 24 million point of sale (POS) terminals accept EMV cards as of Q4 2012. This represents 44.7% of the total payment cards in circulation and 76.4% of the POS terminals installed globally<sup>4</sup>.

There have been a number of historical factors behind the adoption of EMV chip technology in these other countries. The most important factors have been high fraud rates and the cost and reliability of the communications infrastructure. In markets in Western Europe, Australia, Latin America, and Canada the rate of credit card fraud had been much worse than what the U.S. market has historically experienced. These higher fraud rates, plus the lack of low cost, reliable communications at the retail level, led countries to adopt EMV chip technology to enable greater security at the card and offline payments processing at the terminal level. Each of these markets are smaller than the U.S. market, with fewer financial institutions and merchants to convert to chip technology, so the business case to make

<sup>4</sup> "Latest EMVCo Figures Reveal Continued Market Adoption of EMV Technology." EMVCo, Web. May 2012.



191 Clarksville Road  
Princeton Junction, New Jersey 08550 (USA)  
1.800.556.6828  
[www.smartcardalliance.org](http://www.smartcardalliance.org)

the investment in EMV has been very strong. Countries that have implemented EMV chip technology have seen their counterfeit fraud decline by as much as 67%<sup>5</sup>.

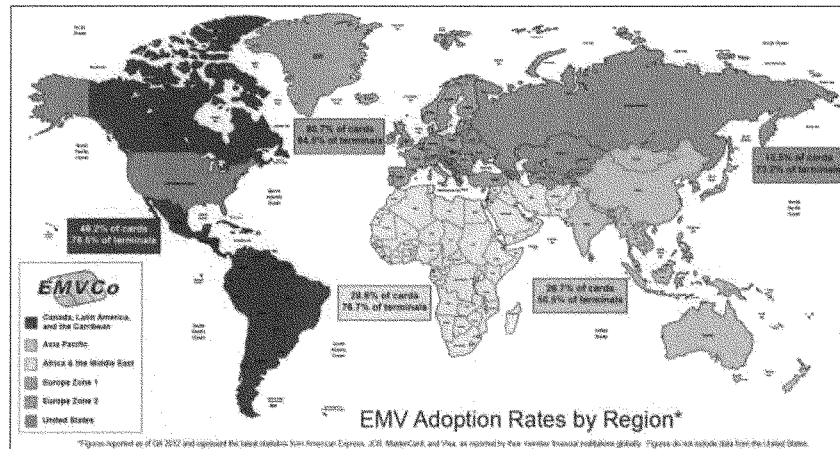


Figure 2: EMVCo map, "EMV Adoption Rates by Region"

[http://www.emvco.com/documents/EMVCo\\_WorldMap2.png](http://www.emvco.com/documents/EMVCo_WorldMap2.png)

The U.S. is one of the last countries to move to EMV chip technology, but has now started its migration. Between July 2011 and June 2012, American Express, Discover, MasterCard and Visa announced plans for moving the U.S. to an EMV-based payments infrastructure. The plans included a series of incentives and policy changes aligning around a target date of October 2015 for card issuers and merchants to complete their implementation of EMV chip cards, terminals and processing systems. ATM operators and retail petroleum outlets were given until 2016 and 2017, respectively, to complete their EMV migrations.

It is important to note that the target dates are not mandates, as U.S. payment brands do not have the ability to set requirements. What they can, and did, was mandate payments processors who connect through their global networks to support EMV chip data in transactions by April 1, 2013. This is the only mandate for U.S. EMV chip implementation.

The payment brands have offered card-issuing financial institutions and merchants an incentive to move to EMV chip technology in the form of a counterfeit fraud liability shift. After the target EMV chip migration dates, the payment brands will shift the responsibility for any fraud resulting from a payment

<sup>5</sup> "Fraud: The Facts." UK Cards Association, Web. 2012.



191 Clarksville Road  
Princeton Junction, New Jersey 08550 (USA)  
1.800.556.6828  
[www.smartcardalliance.org](http://www.smartcardalliance.org)

transaction to the party using the least secure technology. This may be either the issuer of the card or the merchant accepting the payment card.

As an example, if a merchant can accept EMV chip cards and the cardholder presents a magnetic stripe card and there is fraud, the issuer would bear the liability for fraud. Conversely, if a cardholder presents an EMV chip card for payment and the merchant only accepts magnetic stripe cards, the merchant would be liable for any fraud. If both parties have deployed EMV and fraud results from that transaction, the current rules for fraud liability are applied.

This fraud liability shift ensures that those who have made the investment in EMV chip technology will not bear responsibility or cost from fraud from another stakeholder who has not made their system more secure. The goal of the liability shift is to encourage both issuers and merchants to move to EMV technology at the same time so that fraud is removed from the system, not shifted from one party to another.

#### Status of U.S. EMV Migration

The U.S. payments industry is approximately two years into the planned four-year migration to adopt EMV chip technology. Industry stakeholders have been meeting regularly at Smart Card Alliance conferences and EMV Migration Forum meetings and within other industry organizations to address issues that require coordination and cooperation among multiple payments industry participants to ensure a timely and cost effective industry-wide migration to chip technology in the U.S.

The migration to chip cards in the U.S. is complex, expensive and difficult to coordinate. The U.S. market is the largest individual market to convert to chip cards. With over 12,000 financial institutions that issue cards, an estimated 1.2 billion cards in the market, over 10 million POS devices in retail stores, and another 100,000 ATMs installed, the United States payments market is larger than all of Europe's payments markets combined. To date, an estimated 10 to 15 million chip cards have been issued to U.S. consumers, mostly to those who travel frequently outside of the U.S. and who benefit from having the same chip cards that are used in those countries' retail outlets and ATMs. This progress represents less than 2% of the total number of cards in the market. Retailers have replaced approximately 1 million of the more than 10 million POS terminals in stores, but nearly all of these are still operating only as magnetic stripe accepting devices until the software is tested and certified by the acquirers and the stores are ready to begin accepting chip cards.

Implementing EMV chip technology for U.S. debit is also very complex. Complexities result from having 19 debit networks for PIN debit card transactions and the need for compliance with the 2011 Federal Reserve Rulemaking, "Regulation II, Debit Card Interchange Fees and Routing<sup>6</sup>," interpretation of the Durbin Amendment under the Dodd Frank Act. The rulemaking requires that there be at least two unrelated debit card networks supported on each card issued and that merchants have the option to decide which network to route those transactions to each time a debit card is used.

<sup>6</sup>"Regulation II (Debit Card Interchange Fees and Routing)." Federal Reserve System. Web, July 2012.



191 Clarksville Road  
Princeton Junction, New Jersey 08550 (USA)  
1.800.556.6828  
[www.smartcardalliance.org](http://www.smartcardalliance.org)

Accommodating these debit routing rules through agreements among all of the debit networks and the global brands, as well as determining the impact of recent court decisions challenging the Federal Reserve rules, have created uncertainty among issuers and merchants about how to implement EMV chip technology for debit transactions. Today the industry is working on ways to comply with the current rules and still be able to accommodate potential changes that may result from further decisions by the courts, and progress has been made.

#### How EMV Chip Cards Prevent Counterfeit Card Fraud

Chip technology in conjunction with the global EMV payments application standard has proven to be the most effective tool to prevent counterfeit card fraud and maintain the requirements for global interoperability of payment cards for issuers, merchants and consumers. The counterfeit fraud protection comes from two aspects of this technology:

1. The secure storage of the cardholder data inside the chip rather than on a magnetic stripe
2. The dynamic payment transaction data generated by the chip when it is presented to the payment reader for processing the card in a physical retail setting.

The chip itself is a powerful microcomputer with active defenses that prevent tampering with the application and the information it stores inside its memory. Even if chip data were to be copied, it could not be used to create a usable copy onto another chip card because each chip is programmed with a secret key known only to the issuer. The less secure magnetic stripe has no defenses to prevent a criminal from reading the stripe and reprogramming that same card data onto another magnetic stripe, creating an undetectable copy of the original card.

Chip-enabled terminals in retail stores are programmed to pass dynamic security information to the chip before the chip will pass the uniquely generated cryptographic electronic signature to the terminal to complete a payment transaction. This feature is the first line of defense against the use of counterfeit cards that is possible today with magnetic stripe cards.



Figure 3: Chip-enabled POS terminal with an EMV chip card inserted

The chip generates a one time, unique security code, called a cryptogram, for each chip payment transaction that is passed through the chip terminal and through the retailer's POS system and payments processing network. The security cryptogram is verified by the issuer processor to determine that the card used to start the transaction is authentic and that the transaction data was unique to that card. Therefore, a counterfeit copy of that card or a second transaction with the same unique card data would be detected by the issuer and the message normally sent back to the retailer to complete the transaction would deny the transaction.



191 Clarksville Road  
Princeton Junction, New Jersey 08550 (USA)  
1.800.556.6828  
[www.smartcardalliance.org](http://www.smartcardalliance.org)

In addition, EMV chip transactions do not include other data needed for magnetic stripe transactions. This means that any stolen data cannot be used to create a fraudulent transaction in an EMV chip or magnetic stripe environment.

The dynamic data generated by EMV chip cards and the omission of data used in magnetic stripe transactions greatly devalue any payment data that is present in the retailer's or third party processor systems since the chip data cannot be made into counterfeit cards to commit fraud. For example, if EMV chip data had been present in the retailers' systems that were recently victimized by a POS malware attack that extracted card transaction data, the impact of the data breach would have been significantly lessened for the merchant, the card issuers and the consumers through greatly reduced risk of counterfeiting and the resulting card fraud.

The EMV standard also supports additional security mechanisms including the manner with which consumers verify their identities, called Cardholder Verification Methods (CVMs). The EMV standard supports signature, PIN and/or no CVM. Chip-based payment cards that use signature as a CVM have all of the security benefits that the chip and the EMV transaction data provide for protection from counterfeiting and resulting fraud. Chip-based payment cards that use PINs as a CVM provide an added layer of security that prevents the physical card from being used if it is lost or stolen. In the U.S., card issuers will decide which CVMs they want to support based on customer profiles and card management considerations. Merchants can decide which CVMs available on each card they will accept in their retail outlets. As a result, it is likely we will see EMV chip cards issued with a mix of signature, PIN and no CVMs in the U.S.

The issuance of chip cards in the U.S. does not mean the elimination of the magnetic stripe altogether. Financial institutions will continue to issue chip cards with a magnetic stripe on the back for the foreseeable future in order to enable consumers to continue to use these cards at merchant locations that haven't yet upgraded to chip, or in some countries who have not yet adopted the EMV chip standard.

These magnetic stripes that will remain on the backs of bank-issued EMV chip cards do not pose a fraud threat to card issuers or consumers when chip-enabled merchant terminals are widely deployed. When issued on a chip card, a magnetic stripe has different information stored, so when swiped at an EMV chip-accepting terminal, it signals to the terminal that the card was issued with a chip. The terminal will then force the card to be used as a more secure chip card rather than as a less secure magnetic stripe card at that device.

Another scenario is where that chip card's magnetic stripe is copied and a card is created with that card's data written to another magnetic stripe on an unauthorized second card. When that counterfeit card is swiped at a merchant terminal that can process a chip transaction, the terminal would also direct the customer to use the chip. Because the chip doesn't exist on this counterfeit card, the transaction will be declined. If the counterfeit card is used at a terminal that does not support a chip, the card would be accepted unless the issuer flags the transaction based on certain usage analytics or if the cardholder reported the card lost or stolen.



191 Clarksville Road  
Princeton Junction, New Jersey 08550 (USA)  
1.800.556.6828  
[www.smartcardalliance.org](http://www.smartcardalliance.org)

After the fraud liability shift date, if the copied card made with the magnetic stripe data of a chip card is used at a terminal that does not support a chip, and the card is accepted even though it is a copy, the merchant would be responsible for that fraud because it did not have the more secure EMV chip handling capability that would have detected the card was a counterfeit. This is the reason for the liability shift discussed earlier; it's important for both the issuance and acceptance infrastructures to move to chip at the same time to provide the most protection from counterfeit card fraud.

In a third scenario where chip payment card data is intercepted and used to make an online purchase, there are additional security measures that online merchants use, including the three or four digit card security code printed on the card (and which is not available from either the magnetic stripe or the chip), the cardholder's billing address information, or both. Online purchases where the EMV chip is not used in the payment transaction, called Card-Not-Present (CNP) transactions, are not protected by the issuance of EMV chip cards. However, there are other ways to manage CNP fraud risk that are being used today and new technologies that are being developed to address this problem.

To summarize, the security features that EMV chip cards provide to the market in conjunction with the chip reading terminals and advanced payments processing upgrades to support dynamic data are a powerful set of tools to take counterfeit fraud out of the payments system. These security features reduce the likelihood of, or the resulting damage from, any future data breaches against retailers, processors and financial institutions.

#### Conclusion

In summary, the U.S. reliance on magnetic stripe payment cards has made the country a target for fraud. Evidence to support this are: the increasing **attacks** on U.S. retailers, of which the FBI found at least 22 instances in the past year<sup>7</sup>, and the fact that the U.S. is the only region where counterfeit card fraud rises consistently. Hackers are motivated by the big profits that they can make from selling U.S. magnetic stripe payment data on the black market to criminals to make and use counterfeit magnetic stripe cards.

Joining more than 80 countries and implementing EMV chip technology will greatly devalue U.S. payment card data in the eyes of criminals because it cannot be used to create counterfeit chip or magnetic stripe cards. Other countries that implemented EMV chip payments saw fraud decrease by as much as 67%.

While the move to EMV chip payments in the U.S. is a complex and expensive undertaking, it is a critical one that will benefit our entire payments system. I am encouraged by the payments industry's recognition that we need to move EMV chip technology. I am even more encouraged by the fact that many of the largest financial institutions are now issuing EMV chip cards and big retail chains are moving

<sup>7</sup> "Recent Cyber Intrusion Events Directed Toward Retail Firms." FBI Cyber Division. Web, 17 Jan. 2014.



191 Clarksville Road  
Princeton Junction, New Jersey 08550 (USA)  
1.800.556.6828  
[www.smartcardalliance.org](http://www.smartcardalliance.org)

quickly to put in place the chip-enabled terminals and working with their acquirer processors to enable those devices to begin accepting chip transactions by the October 2015 targeted completion dates.

**Contact Information:**

Randy Vanderhoof  
Executive Director  
Smart Card Alliance  
191 Clarksville Road  
Princeton Junction, NJ 08550  
[www.smartcardalliance.org](http://www.smartcardalliance.org)  
609-587-4208  
[rvanderhoof@smartcardalliance.org](mailto:rvanderhoof@smartcardalliance.org)

*Randy Vanderhoof, Director  
EMV Migration Forum  
[www.emv-connection.com/emv-migration-forum/](http://www.emv-connection.com/emv-migration-forum/)*



191 Clarksville Road  
Princeton Junction, New Jersey 08550 (USA)  
1.800.556.6828  
[www.smartcardalliance.org](http://www.smartcardalliance.org)

## Appendix 1: About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. The Alliance invests heavily in education on the appropriate uses of technology for identification, payment and other applications and strongly advocates the use of smart card technology in a way that protects privacy and enhances data security and integrity. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart card technology, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America.

The Alliance is comprised of more than 220 member companies worldwide, including participants from financial, government, enterprise, transportation, mobile telecommunications, healthcare and retail industries. A mix of issuers and adopters of smart card technology work in concert with leading industry suppliers of the full range of products and services supporting the implementation of smart-card based systems for secure payments, identification, access and mobile communications.

The four main priorities of the Alliance are:

- To influence standards that are relevant to smart card adoption and implementation;
- To maintain a voice in public policy that affects smart card adoption and implementation;
- To serve as an educational resource to its members and the industry; and
- To provide a forum for cutting edge discussions and projects on issues surrounding smart cards.

Within the Smart Card Alliance organization, members have addressed the market requirements and technical applications for smart cards in specific industry verticals by forming industry councils. Six active councils in 2013 each worked from a specific charter and mission statement. Over 500 individuals from 127 organizations supported these councils, with many participating in more than one council. The Identity Council, Access Control Council, and Health and Human Services Council attend to the identity management and security uses of smart cards including security badges, digital log in credentials, and approaches to secure networks and Internet services. The Payments and Transportation Councils serve the payments markets for bank cards, prepaid cards, and transit fare payment systems. The Mobile and NFC Council has the most cross-industry role, since mobile technology and NFC are affecting payments, identity and access applications across many new mobile platforms.



191 Clarksville Road  
Princeton Junction, New Jersey 08550 (USA)  
1.800.556.6828  
[www.smartcardalliance.org](http://www.smartcardalliance.org)

## Appendix 2: About the EMV Migration Forum

Launched in August 2012, the EMV Migration Forum – a cross-industry organization that is separate but affiliated with the Smart Card Alliance – focuses on supporting the EMV implementation steps required for global and regional payment networks, issuers, processors, merchants and consumers to help ensure a successful introduction of more secure EMV chip technology in the United States. The Forum mission is to address topics that require some level of industry cooperation and/or coordination to migrate successfully to EMV technology in the United States. By establishing a professional, collaborative environment for engaged discussion and debate among all industry stakeholders, the organization is harnessing the collective expertise of the U.S. payments industry to guide migration to more secure EMV technology.

The Forum now has more than 150 member organizations, with representatives from all industry stakeholder groups – payment brands, issuers, acquirer processors, merchants, debit networks and industry suppliers.

Over 400 individuals from more than 100 member organizations are involved in the Forum's six Working Committees, which are chaired by industry leaders and meet via regular conference calls and at in person member meetings.

In 2013, Forum members met a total of nine times in person, from two-day all-member conferences to one-day in-person Working Committee meetings. Each participating organization sends its top payments experts and managers to share information and collaborate on creative solutions to the challenges ahead for the U.S. migration to EMV.

The Forum has been successful in dealing with such challenging issues as EMV debit routing, certification testing, and changes impacting ATM operators, merchants, and card issuers in a congenial, courteous and professional environment for the benefit of all involved.



191 Clarksville Road  
Princeton Junction, New Jersey 08550 (USA)  
1.800.556.6828  
[www.smartcardalliance.org](http://www.smartcardalliance.org)

## Appendix 3: References/Resources

"Card Payments Roadmap in the U.S.: How Will EMV Impact the Future Payments Infrastructure?," Smart Card Alliance Payments Council white paper, January 2013, <http://www.emv-connection.com/card-payments-roadmap-in-the-u-s-how-will-emv-impact-the-future-payments-infrastructure/>

Card-Not-Present Fraud: A Primer on Trends and Transaction Authentication Processes, Smart Card Alliance Payments Council white paper, February 2014, <http://www.emv-connection.com/card-not-present-fraud-a-primer-on-trends-and-transaction-authentication-processes/>

EMV Connection web site, <http://www.emv-connection.com>

"The EMV Ecosystem: An Interactive Experience for the Payments Community," Smart Card Alliance resource, February 2013, <http://www.emv-connection.com/the-emv-ecosystem-an-interactive-experience-for-the-payments-community/>

EMV Frequently Asked Questions, Smart Card Alliance publication, <http://www.emv-connection.com/emv-faq/>

"EMV 101: Fundamentals of EMV Chip Payment," EMV Migration Forum webinar, January 2014

"EMV Testing and Certification White Paper: Current U.S. Payment Brand Requirements for the Acquiring Community," EMV Migration Forum white paper, July 2013

"Large Scale Payment Data Breaches Highlight Need for U.S. Card Issuers and Retailers to Move More Quickly to Smart Chip Payment Technology," Smart Card Alliance brief, January 2014

Smart Card Alliance web site, <http://www.smartcardalliance.org>

"Standardization of Terminology," EMV Migration Forum publication, February 2014, <http://www.emv-connection.com/standardization-of-terminology/>



191 Clarksville Road  
Princeton Junction, New Jersey 08550 (USA)  
1.800.556.6828  
[www.smartcardalliance.org](http://www.smartcardalliance.org)

**Randy Vanderhoof's Bio**

**Randy Vanderhoof** is the **Executive Director** of the **Smart Card Alliance**. The Smart Card Alliance is a not-for-profit, multi-industry association of over 200 member firms working to accelerate the widespread acceptance of smart card technology in North America and Latin America. In addition to his leadership role with the Smart Card Alliance, in August 2012 he became the **Director** of the **EMV Migration Forum**, an independent, cross-industry organization established to support the alignment of the EMV implementation steps required for global payment networks, regional payment networks, issuers, processors, merchants, and consumers to successfully move from magnetic stripe technology to secure EMV contact and contactless technology in the United States.

Chairman BROUN. Mr. Vanderhoof, thank you so much. I think we have time for one more.

Mr. Brookman, if you would please limit it to five minutes and then we will recess and come back right after votes. We have eight more minutes before the clock runs out, and as Members know, it will be held open for a while.

So, Mr. Brookman.

**TESTIMONY OF MR. JUSTIN BROOKMAN,  
DIRECTOR, CONSUMER PRIVACY,  
CENTER FOR DEMOCRACY & TECHNOLOGY**

Mr. BROOKMAN. Absolutely. Thank you, Chairman Broun, Chairman Bucshon, Ranking Members Maffei and Lipinski. Thank you very much for the opportunity to testify here today.

I am here today on behalf of the Center for Democracy & Technology. We are a digital rights advocacy group based here in D.C. and I head up our work on commercial data privacy. Some of us like me are lawyers but we also have technologists on staff who focus on internet architecture, encryption, and cybersecurity.

We have been concerned about the issue of data security for some time. We have supported state efforts to require notification to consumers in the event of data breach, and we have encouraged the Federal Trade Commission to aggressively pursue bad data security cases under its general commercial protection authority.

Unfortunately, it appears that the current policy solutions in place have been insufficient to staunch the proliferation of personal data breach. Just last week, the FTC announced that identity theft was the number one source of consumer complaints for the 14th year in a row. Moreover, the problem seems to be getting worse and not better. For one thing, there is more and more attack surface for malicious actors to target. Even the food trucks where I get my lunch every day accept credit card payments through smart readers attached to their phones. And people increasingly use credit cards for \$1 and \$2 purchases due to improvements in technology and purchase flows.

The proliferation of financial account usage is of course tied to the bigger issue of big data in general. It is now easier for companies to collect and analyze all sorts of information about us, not just based on how we use their services but possibly supplemented by third-party data brokers as well. And it is cheaper for them to maintain these files, too. As storage technology advances, it is just simpler to keep old data around forever.

And it is notable that Target was the subject of what was possibly the largest data breach in history because Target had been discussed in privacy circles recently for different reasons. Last year, it was revealed that Target was developing very sensitive predictive analytics technologies about the people who shop there, analyzing what they bought to develop profiles about what sort of people they were. And the most famous story coming out of that was there was a father who stormed into Target one afternoon complaining his daughter was receiving pregnancy-related coupons from Target, for diapers or prenatal vitamins, and he said how dare they; she is just a teenager, and then comes back a couple

days later and apologizes that it turns out Target was right in this particular case.

It is worth noting that this sort of sensitive information, information about what we buy, what we read, where we go, who we associate with, that is at risk, too, in the big data world. Target didn't just lose information about 40 million financial accounts; they also allegedly lost 70 million profiles from its customer relationship management database. Did that include in there assessments of all their shoppers possibly supplemented with third-party data? We don't know.

We believe these issues should be addressed together. First, the United States should have comprehensive data privacy and security legislation. We are one of the few developed nations in the world that doesn't have baseline protections for all personal information. The FTC has tried to use its limited general consumer protection mandate to better protect privacy and data security, but that authority is currently being challenged in court by Wyndham Hotels. In that case, the FTC argued that Wyndham Hotels' use of objectively poor data security to safeguard consumer data constituted an unfair business practice under Section 5 of the FTC Act. Wyndham has refused to accept responsibility for its poor security management and is challenging the FTC's authority to go after bad security practices.

We believe technology has a really important role to play in limiting data breach incidents, but we do not believe that Congress should enact specific technological data security solutions. That would embed current practices in the law and limit innovation in the future. Rather, policymakers should enact laws that strongly incentivize companies to safeguard personal data with significant consequences for companies that fail to use reasonable security practices.

Now, for financial account information, there are some actually pretty good incentives under the law right now. Companies who undergo a financial data breach have to absorb the cost of data breach notification to consumers, investigation, credit monitoring, loss to consumer goodwill, and then payment to the issuing bank for potential violation of PCI standards.

Yesterday, it was reported that Target has already spent over \$60 million in the breach from last year, and in 2007, TJX Corporation reported that they had spent over \$250 million from their data breach incident.

However, it is not clear that these potential costs are sufficiently internalized today within corporate decision-making. Organizations and people in general unfortunately have a tendency to underestimate small percentage chances of very bad things happening. And that appears to be what is happening with data security. Companies are convincing themselves it won't happen to them, and there are many cases failing to adequately account for security risks.

We believe that strengthening the FTC's authority to go after bad security practices along with the authority to obtain civil penalties for bad security would help push companies in the right direction. We also believe that legislation should require companies to develop privacy and security plans and to adhere to privacy and

security-by-design principles. The companies are encouraged to think proactively and prophylactically about data privacy and security from the very beginning of product and system development that will result in better outcomes for all consumers.

Thank you very much for the opportunity to testify and I look forward to your questions.

[The prepared statement of Mr. Brookman follows:]



KEEPING THE INTERNET  
OPEN • INNOVATIVE • FREE

[www.cdt.org](http://www.cdt.org)

1634 I Street, NW  
Suite 1100  
Washington, DC 20006

P +1-202-637-9800  
F +1-202-637-0968  
E [info@cdt.org](mailto:info@cdt.org)

Statement of **Justin Brookman**  
*Director, Consumer Privacy*  
*Center for Democracy & Technology*

Before the House of Representatives  
Committee on Science, Space, and Technology

## **CAN TECHNOLOGY PROTECT AMERICANS FROM INTERNATIONAL CYBERCRIMINALS?**

**March 4, 2014**

On behalf of the Center for Democracy & Technology (CDT), I thank you for the opportunity to testify today. CDT welcomes the attention the Committee has given to the pressing issues of consumer data privacy and security, especially in the context of the recent high-profile breaches that have affected a range of businesses and educational institutions.

CDT is a non-profit, public interest organization dedicated to preserving and promoting openness, innovation, and freedom on the Internet. I currently serve as the Director of CDT's Consumer Privacy Project. Our project focuses on issues surrounding consumer data, and I have previously testified before Congress on the issues of data breach, privacy, and security.

CDT's testimony today will briefly describe the impact on businesses and consumers of data breach and malicious access. I will then describe the existing legal framework covering data security, including the recently released federal cybersecurity guidelines. I will conclude with thoughts on suggested reforms – both legal and technical – that would more effectively protect consumer privacy and security. Ultimately, Congress can best protect consumer information by strengthening legal incentives for companies to better safeguard data, and by enacting comprehensive data privacy legislation to give users more insight and control over how their information is collected and used.

### **I. The Expanding Cost to the Economy of Data Breach**

As recent events have demonstrated, data breaches can be quite broad in scope. Target reported that its 2013 data breach could have affected up to 110 million customers.<sup>1</sup> Neiman Marcus reported in January 2014 that unauthorized hackers had breached its servers, accessing the payment information of its own

<sup>1</sup> Jia Lynn Yang & Amrita Jayakumar, *Target Says Up to 70 Million More Customers were Hit by December Data Breach*, WASH. POST (Jan. 10, 2014), available at [http://www.washingtonpost.com/business/economy/target-says-70-million-customers-were-hit-by-dec-data-breach-more-than-first-reported/2014/01/10/0ada1026-79fe-11e3-8963-b4b654bcc9b2\\_story.html](http://www.washingtonpost.com/business/economy/target-says-70-million-customers-were-hit-by-dec-data-breach-more-than-first-reported/2014/01/10/0ada1026-79fe-11e3-8963-b4b654bcc9b2_story.html).

customer base.<sup>2</sup> That same month, Michael's disclosed that its systems holding customer data may have been breached.<sup>3</sup> And just last month, the University of Maryland suffered a security attack affecting records containing personally identifiable information (including names, dates of birth, and Social Security Numbers) of faculty, staff, and students dating back to 1998.<sup>4</sup> Unfortunately, data breaches are not a new problem. In May 2011, I testified in the House Energy and Commerce Committee on the data breach issue following two high profile breaches that affected Sony Corp. and Epsilon, a major email marketing firm.<sup>5</sup> Those breaches, combined, affected a total of over 160 million accounts.<sup>6</sup> According to the Privacy Rights Clearinghouse, over 660 million records have been breached in approximately 4200 incidents since 2005.<sup>7</sup>

Data breaches impose substantial financial costs on businesses and consumers and also undermine consumer confidence. According to a 2013 Ponemon Institute Study, the average cost that a U.S. company incurs as a result of a data breach is \$5.4 million per incident.<sup>8</sup> That does not count the cost to consumers. Consumers whose personal information is lost or stolen in data breaches face increased risks of identity theft, spam and phishing attacks, and sometimes humiliating loss of privacy over sensitive medical conditions. They also lose trust in the services on which they depend, which hurts both the consumers and those businesses.

There are few options for consumers who seek to avoid breaches (other than using cash for all transactions, which is not very feasible). After a breach is reported, it is often not clear what consumers can do to mitigate the consequences, especially as data breach notifications can be difficult to parse. The typical remedy – free credit reporting monitoring for a year or more – is focused on fixing a problem after it occurs rather than prospectively defending against unauthorized use of consumer data.

<sup>2</sup> Hayley Tsukayama, *Neiman Marcus Confirms Data Breach, Some Customers at Risk*, WASH. POST (Jan. 11, 2014), available at [http://www.washingtonpost.com/business/technology/neiman-marcus-confirms-data-breach-offers-few-details/2014/01/11/56c6dc7e-7ae1-11e3-af7f-13bf0e9965f6\\_story.html](http://www.washingtonpost.com/business/technology/neiman-marcus-confirms-data-breach-offers-few-details/2014/01/11/56c6dc7e-7ae1-11e3-af7f-13bf0e9965f6_story.html).

<sup>3</sup> Hayley Tsukayama, *Michaels Discloses Possible Customer Data Breach; Secret Service Investigating*, WASH. POST (Jan. 27, 2014), available at [http://www.washingtonpost.com/business/technology/michaels-discloses-possible-customer-data-breach-secret-service-investigating/2014/01/27/73a8538e-877c-11e3-a5bd-844629433ba3\\_story.html](http://www.washingtonpost.com/business/technology/michaels-discloses-possible-customer-data-breach-secret-service-investigating/2014/01/27/73a8538e-877c-11e3-a5bd-844629433ba3_story.html).

<sup>4</sup> Patrick Svitek, *University of Maryland Offers Four More Years of Credit Monitoring for Security Breach Victims*, WASH. POST (Jan. 27, 2014), available at [http://www.washingtonpost.com/local/university-of-maryland-offers-4-more-years-of-credit-monitoring-for-security-breach-victims/2014/02/25/16e65e9a-9e72-11e3-a050-dc3322a94fa7\\_story.html](http://www.washingtonpost.com/local/university-of-maryland-offers-4-more-years-of-credit-monitoring-for-security-breach-victims/2014/02/25/16e65e9a-9e72-11e3-a050-dc3322a94fa7_story.html).

<sup>5</sup> Testimony of Justin Brookman, Center for Democracy & Technology, United States House of Representatives Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade (May 4, 2011), available at [https://www.cdt.org/files/pdfs/20110504\\_bonomack\\_jb.pdf](https://www.cdt.org/files/pdfs/20110504_bonomack_jb.pdf).

<sup>6</sup> Ian Sherr, *Hackers Breach Second Sony Service*, WALL ST. J. (May 2, 2011), available at <http://online.wsj.com/article/SB10001424052748704436004576299491191920416.html?mod=e2tw>; Les Luchter, *Epsilon Confronts Possible \$225M In Data Breach*, MediaPost News (April 29, 2011), [http://www.mediapost.com/publications/?fa=Articles.showArticle&art\\_aid=149603](http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=149603).

<sup>7</sup> Privacy Rights Clearinghouse, *Chronology of Data Breaches*, last updated February 27, 2014, <http://www.privacyrights.org/data-breach/new>.

<sup>8</sup> Ponemon Institute, "2013 Cost of Data Breach Study: Global Analysis" (May 2013), available at [https://www4.symantec.com/mktginfo/whitepaper/053013\\_GL\\_NA\\_WP\\_Ponemon-2013-Cost-of-a-Data-Breach-Report\\_daiNA\\_cta72382.pdf](https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf).

## II. More Companies, Collecting More Data

Companies also face difficulties in mitigating or avoiding the risk of security breaches. As more companies collect information in ever increasing ways through online commerce, mobile applications, and wearable devices, an increasing number of businesses are creating databases containing personal data. This means that more companies than ever before are tempting targets for hackers seeking to gain access to personal data; those companies that have not historically been prime targets for data breach may not be prepared for unauthorized third party access or its consequences. The interaction between hackers and businesses can at times resemble an arms race, with each side seeking to increase its capabilities to conduct or resist a breach.

As more businesses collect consumer data – whether through mobile applications, networked devices in the home, or ecommerce sites – data security has become an increasingly important issue for many companies that may have had little to no prior experience with creating security programs. Moreover, some companies may share data they collect with third parties, requiring reasonable security standards for the transmission of data outside of the company. As some companies may not yet have developed security programs that can withstand attacks by outsiders seeking to gain unauthorized access, the risk of data breach remains high.

One factor driving the increased collection of consumer data is the promise of “Big Data.” Big data refers to datasets whose size is beyond the ability of traditional software tools to capture, store, manage, and analyze.<sup>9</sup> The big data trend includes not only the ongoing, exponential expansion of data collection, but also advances in computing power, storage, and the ability to analyze separate datasets. The spread of these developments has been rapid and broad.<sup>10</sup>

While big data holds a great deal of promise, it also requires strong security measures. As CDT has argued, any collection of personal data by companies implicates individual privacy interests.<sup>11</sup> Collection and retention by themselves open up companies to potential hazards – and not just from data breaches. The risk of unauthorized access by company employees, changes in company practices, and illegitimate government access all implicate individual privacy interests.

Given the widening scope of commercial data collection and the growing scale and frequency of data breaches, it is appropriate to question whether enough is being done to solve the problem. Although state and federal laws require companies to notify affected consumers of a data breach, the financial and reputational costs of notification may not provide some companies with adequate incentive to properly protect consumers’ data. The goal of federal policy should be to

<sup>9</sup> James Manyika et al., *Big Data: The Next Frontier for Innovation, Competition, and Productivity*, McKinsey Global (May 2011), [http://www.mckinsey.com/Insights/MGI/Research/Technology\\_and\\_Innovation/Big\\_data\\_The\\_next\\_frontier\\_for\\_innovation](http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Big_data_The_next_frontier_for_innovation).

<sup>10</sup> For example, in 2012, Microsoft announced that Excel, part of the basic Office suite of software and a program used by many millions, will include big data analytic capabilities. *Microsoft Seeks an Edge in Analyzing Big Data*, N.Y. TIMES (Oct. 29, 2012), at B2, available at <http://www.nytimes.com/2012/10/30/technology/microsoft-renews-relevance-with-machine-learning-technology.html>.

<sup>11</sup> Justin Brookman & G.S. Hans, *Why Collection Matters: Surveillance as a De Facto Privacy Harm*, Future of Privacy Forum Big Data & Privacy Workshop Paper Collection (2013), available at <http://www.futureofprivacy.org/wp-content/uploads/Brookman-Why-Collection-Matters.pdf>.

incentivize both companies and government bodies to install sufficient front-end data security measures, to minimize their holdings of consumer data that is no longer necessary for a specific, legitimate purpose, and to develop structures that monitor and control where consumer data resides, without impeding innovation. Cybersecurity policy should promote substantive protections, but avoid prescribing specific technical requirements. Finally, although data breach is an important problem, new rules on data security would be best addressed as part of comprehensive baseline consumer privacy legislation.

### III. The Existing Legal Framework for Security and Data Breach Notification

At the federal level, there are several sectoral laws and regulations requiring entities holding personal information to adopt reasonable security measures and, sometimes, notification to the victims of data breach. The federal laws are something of a patchwork insofar as they cover some data in certain contexts, but not others, reflecting the sector-by-sector approach Congress has thus far taken with regard to privacy rules. For example, the Federal Information Security Management Act (FISMA),<sup>12</sup> the Privacy Act,<sup>13</sup> and the Veterans Affairs Information Security Act<sup>14</sup> apply to the federal sector, but not the private sector. The Fair Credit Reporting Act (FCRA) applies to consumer reporting agencies,<sup>15</sup> the Gramm-Leach Bliley Act (GLBA) applies to covered financial institutions,<sup>16</sup> and the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) apply to covered health care entities.<sup>17</sup> Consumer data that is not covered under these laws is generally protected under the Federal Trade Commission (FTC) Act.<sup>18</sup>

Section 5 of the FTC Act prohibits deceptive and unfair practices in interstate commerce.<sup>19</sup> Although the FTC Act does not provide for notification to consumers in the event of a data breach, the FTC has used its unfairness authority to bring suits against companies for failing to adopt reasonable security procedures. Since 2004, the FTC has settled dozens of data security cases against companies that it alleged had failed to provide reasonable and appropriate protections for consumers' information.<sup>20</sup> The settlements have included cases involving traditional data security in the context of records containing personally identifiable information,<sup>21</sup> to newer technologies such as Internet-enabled video cameras that allowed consumers to monitor their homes remotely allowed unauthorized users to tap into the camera feeds.<sup>22</sup>

<sup>12</sup> 44 U.S.C. 3541 et seq.

<sup>13</sup> 5 U.S.C. 552a et seq.

<sup>14</sup> 38 U.S.C. 5722 et seq.

<sup>15</sup> 15 U.S.C. 1681 et seq.

<sup>16</sup> 15 U.S.C. 6801 et seq.

<sup>17</sup> 42 U.S.C. 1320d et seq.

<sup>18</sup> 15 U.S.C. 45(a) et seq.

<sup>19</sup> *Id.*

<sup>20</sup> Commission Statement Marking the FTC's 50th Data Security Settlement, Jan. 31, 2014, available at <http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf>.

<sup>21</sup> *GMR Transcription Servs., Inc.*, Matter No. 112-3120 (F.T.C. Dec. 16, 2013) (proposed consent order), available at <http://www.ftc.gov/news-events/press-releases/2014/01/provider-medical-transcript-services-settles-ftc-charges-it>.

<sup>22</sup> *TRENDnet, Inc.*, No. 122-3090 (Sept. 4, 2013), available at <http://www.ftc.gov/opa/2013/09/trendnet.shtm>.

The FTC's ability to use its Section 5 authority to require reasonable security practices is currently being litigated in the U.S. District Court in New Jersey. The case, *FTC v. Wyndham*, concerns the security practices of the Wyndham hotel chain, which suffered three security breaches between 2008 and 2010.<sup>23</sup> The FTC filed a complaint against Wyndham in 2012 alleging that the company's security practices — including failing to encrypt payment data and the use of default logins and passwords — constituted unfair and deceptive practices under the FTC Act. However, rather than settling as most defendants do, Wyndham took the somewhat unusual step of challenging the FTC's case, and has moved to dismiss the case. The thrust of Wyndham's argument is that the FTC Act does not explicitly cover data security practices, and that the many subsequent bills introduced in Congress that would grant the FTC explicit, specific authority to regulate data security practices implicitly indicate that Congress did not intend to grant such authority under the FTC Act. CDT disagrees with Wyndham's argument on multiple grounds.<sup>24</sup> The continued recurrence of data breaches demonstrates the importance of the FTC's ability to regulate data security by bringing enforcement actions against companies with subpar security practices.

As of early 2014, 46 states, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have enacted legislation on the breach of personal information.<sup>25</sup> There are also several federal laws requiring notification to consumers in the event of a data breach. Although the state standards vary and the federal laws are incomplete in their coverage, most companies already do notify affected individuals in the event of a data breach. The great majority of data breach law focuses on notifying consumers after a data breach, without providing incentives or requirements regarding data collection and retention that could help prevent data breaches from occurring in the first place.

Each of the state laws provides a general time frame in which the compromised entity must notify consumers of a breach. Often, this time frame is defined as **within** the most expedient time possible and without unreasonable delay. Some states — such as New York<sup>26</sup> and Texas<sup>27</sup> — levy civil or criminal penalties on compromised entities if they fail to promptly notify consumers of a breach, while other states — such as California<sup>28</sup> — do not. Some states — such as California,<sup>29</sup> but not New York or Texas — allow individuals to bring a private right of action for injuries suffered as a result of violations of the breach notification law. Many states — including California,<sup>30</sup> New York<sup>31</sup> and Texas<sup>32</sup> — provide for some exemption from breach notification requirements when breached private information is encrypted.

<sup>23</sup> Federal Trade Commission v. Wyndham Worldwide Corporation, et al., Docket No. Case No. 2:12-cv-01365-SPL, (June 26, 2012) (complaint), available at <http://www.ftc.gov/sites/default/files/documents/cases/2012/06/120626wyndamhotelscmpt.pdf>.

<sup>24</sup> G.S. Hans, *Data Security and Your Next Hotel Stay: How the FTC Encourages Strong Security Practice*, Cen. Dem. Tech. PolicyBeta Blog (May 21, 2013), <https://www.cdt.org/blogs/gs-hans/2105data-security-and-your-next-hotel-stay-how-ftc-encourages-strong-security-practice>.

<sup>25</sup> National Conference of State Legislatures, *Security Breach Notification Laws* (last updated January 21, 2014), <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.

<sup>26</sup> N.Y. Gen. Bus. Law 899-aa(d)(6).

<sup>27</sup> Tex. Bus. & Com. Code 521.151.

<sup>28</sup> Cal. Civ. Code 56.06, 1785.11.2, 1798.29, 1798.82.

<sup>29</sup> Cal. Civ. Code 1798.84(b).

<sup>30</sup> Cal. Civ. Code 1798.82(e).

#### IV. Federal Cybersecurity Policy

The Obama administration has given some guidance to companies to promote security against cyber attacks. In February 2014, the National Institute of Standards and Technology (NIST) released its Framework for Improving Critical Infrastructure Cybersecurity, pursuant to Executive Order 13636.<sup>33</sup> The framework is designed to promote security for critical infrastructure within the United States, while simultaneously taking into account business considerations and privacy and civil liberties concerns.

During the process leading up to adoption of the Framework, CDT, along with fourteen other organizations, submitted comments to NIST calling for the inclusion of privacy protections based on the Fair Information Practice Principles (FIPPs) in the final Framework.<sup>34</sup> The FIPPs have been used for decades to effectively and flexibly promote privacy. In the drafting process, NIST had acknowledged the importance of the FIPPs, in a proposed Appendix to the draft Framework. Some commenters, however, encouraged NIST to use process-based protections, rather than the substantive protections offered by the FIPPs.<sup>35</sup> In its final Framework, NIST adopted a modified process-based approach. Rather than specifying at some level of detail how FIPPs could be applied to cybersecurity measures, the Framework adopts the process-based orientation for the most part.<sup>36</sup> It calls on organizations to assess the privacy implications of their cybersecurity programs, to have privacy-trained personnel, and to put in place processes to ensure that cybersecurity activities are lawful.

CDT supports the use of the Framework to help companies that want to more effectively secure their data from unauthorized access. However, the Framework's process-based approach gives less guidance to companies and less protection to consumers than is needed. CDT hopes that the Framework will encourage companies to consider strong privacy and security protections, ideally based on the FIPPs, when determining how to promote cybersecurity. Effective and robust security programs to guard against unauthorized data breach are necessary in order to both protect critical infrastructure and protect consumer privacy and data security.

#### V. Legal and Technical Solutions

Rather than prescribing specific technologies, Congress should enact legislation to sufficiently incentivize companies to implement innovative solutions to minimize data breach. At the very

---

<sup>31</sup> N.Y. Gen. Bus. Law 899-aa(b).

<sup>32</sup> Tex. Bus. & Com. Code 521.053(a).

<sup>33</sup> National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014), *available at* <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>.

<sup>34</sup> Letter from Access et al. to Adam Sedgewick, Nat'l Institute of Standards & Tech. (Dec. 13, 2013) (on file with author), *available at* [https://www.aclu.org/sites/default/files/assets/preliminary\\_cybersecurity\\_framework\\_comments\\_-\\_privacy\\_and\\_civil\\_liberties\\_coalition.pdf](https://www.aclu.org/sites/default/files/assets/preliminary_cybersecurity_framework_comments_-_privacy_and_civil_liberties_coalition.pdf).

<sup>35</sup> Letter from Harriet P. Pearson, Partner, Hogan Lovells US LLP, to Adam Sedgewick, Nat'l Institute of Standards & Tech. (Dec. 5, 2013) (on file with author), *available at* [http://csrc.nist.gov/cyberframework/framework\\_comments/20131205\\_harriet\\_pearson\\_hoganlovells.pdf](http://csrc.nist.gov/cyberframework/framework_comments/20131205_harriet_pearson_hoganlovells.pdf).

<sup>36</sup> The framework does indicate that, "organizations may consider how, in circumstances in which such measures are appropriate, their cybersecurity program might incorporate privacy principles" such as data minimization, use limitations, transparency, individual consent, redress for adverse impacts, data quality and security, and accountability and auditing measures. *Supra* note 33, at 16.

least, Congress should specifically empower the Federal Trade Commission to continue to bring actions against companies that fail to deploy reasonable security to safeguard consumer data. That use of its Section 5 authority is currently being challenged in the previously discussed *Wyndham* litigation; an adverse decision for the FTC in that case could mean that most companies bear little to no statutory liability for poor data security practices. CDT also supports granting the FTC the ability to seek civil penalties for initial violations of the FTC Act, which it currently lacks.<sup>37</sup> At present, the FTC can only seek civil penalties for data security violations with regard to children's online information under COPPA or credit report information under the FCRA or when a company violates an administrative order. If the agency could seek penalties for an initial violation, it would create a more effective deterrent effect for companies and encourage the adoption of more robust security programs.

CDT also supports the FTC's call for rulemaking authority under the Administrative Procedure Act.<sup>38</sup> Fears about requiring companies to use specific technologies are certainly warranted; CDT has long preferred to focus on best practices and strong privacy and security standards based in large part on Fair Information Practice Principles. Such regulations should give companies some flexibility in promoting consumer privacy and security. Requiring companies to adopt reasonable security standards – such as the creation, auditing, and maintenance of a comprehensive and robust security program – rather than specific technologies, would better protect consumers without relying upon a single technology to serve as a panacea.

With stronger legal incentives in place, industry will give further attention should be given to practical measures that companies can take in order to effectively promote data security and discourage data breaches. In the wake of the Target breach, for example, there were renewed calls for the adoption in the U.S. of the "chip and PIN" standard for credit cards.<sup>39</sup> In the United Kingdom, for example, credit cards contain a microchip (rather than the U.S. standard magnetic stripe), and customers input a PIN in order to complete the transaction. Such solutions deserve further study to determine if they are an appropriate security solution.<sup>40</sup>

In general, however, security cannot be thought of as a product that an organization or firm procures and then neglects, like other aspects of business operations. Security must be a practice that focuses on "defense in depth" and must be a resonating cultural element of the organization. For example, people living in cities have over time learned to take precautions such as locking the doors to their home when they leave. This practice is based on experience of those that have been burgled and people incorporating that experience into their routine. Encrypting data at rest, separating functional networks (e.g., an enterprise network versus the

<sup>37</sup> *Id.*

<sup>38</sup> Testimony of Chairwoman Edith Ramirez, Federal Trade Commission, United States House of Representatives Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade (Feb. 5, 2014), available at [http://www.ftc.gov/system/files/documents/public\\_statements/prepared-statement-federal-trade-commission-protecting-consumer-information-can-data-breaches-be/140205databreaches.pdf](http://www.ftc.gov/system/files/documents/public_statements/prepared-statement-federal-trade-commission-protecting-consumer-information-can-data-breaches-be/140205databreaches.pdf); G.S. Hans, *Target and Neiman Marcus Testify on Data Breach – But What Reforms Will Result?*, Cen. Dem. Tech. PolicyBeta Blog (Feb. 7, 2013), <https://www.cdt.org/blogs/gs-hans/0702target-and-neiman-marcus-testify-data-breach—what-reforms-will-result>.

<sup>39</sup> Alan Yu, *Outdated Magnetic Strips: How U.S. Credit Card Security Lags*, NPR All Tech Considered (Dec. 19, 2013, 5:34 PM), <http://www.npr.org/blogs/alltechconsidered/2013/12/19/255558139/outdated-magnetic-strips-how-u-s-credit-card-security-lags>.

<sup>40</sup> Abigail Wang, *Smart Chip Cards Wouldn't Have Saved Target*, PCMag (Jan. 30, 2014, 12:27 PM), <http://securitywatch.pcmag.com/internet-crime/320071-smart-chip-credit-cards-wouldn-t-have-saved-target>.

operations and maintenance network for point-of-sale devices), and more adversarial policing of network internals in search of insider exploits are examples of “defense in depth” security practices that are not well incorporated into many businesses that do not regularly deal with highly sensitive data – and even those that do have a hard time with these techniques.

Another possible security measure that could be effective in limiting future data breaches is the use of disposable credit card numbers. The security company Abine, for example, has developed a product called MaskMe, which allows customers to create a one-time only credit card number tied to their actual credit card account.<sup>41</sup> Therefore, if unauthorized individuals obtained access to the record of a financial transaction conducted using a MaskMe credit card number, they would not be able to use the credit card number to commit a fraudulent transaction, since the MaskMe number could only be used once. Credit card vendors such as Citi are also beginning to offer similar solutions directly. While it is currently easier to deploy disposable numbers for online transactions, some mobile wallet applications for smart phones (such as Google Wallet) have evolved to offer similar functionality at brick-and-mortar stores.

We are skeptical that enacting federal data breach notification legislation by itself will be effective in curtailing future data breaches. As noted above, nearly all the states already have data breach notification requirements in place. While we are sympathetic to companies’ desire for uniformity of notification requirements, it should be noted that one of the primary benefits of notification requirements is to embed strong incentives to companies to avoid the significant costs of issuing data breach notifications. Merely simplifying the rules for breach notification weakens those incentives by making breach notifications less expensive to issue. If Congress does enact federal breach notification requirements, we strongly urge that such legislation is at least as strong as the best laws in place at the state level. If a federal law were to preempt state laws and replace them with a weak notification regime, the result would be a significant step backwards for consumers and data security. Moreover, federal preemption provisions should explicitly exclude general application consumer protection laws, and should only preempt state laws that govern the data elements covered by the federal statute. States should be free to enact protections for data not covered by federal law. For further recommendations on how to craft federal data breach notification legislation, please refer to the detailed proposals contained in our testimony before the Energy and Commerce Committee in 2011.<sup>42</sup>

## **VI. Future Data Breach and Security Proposals Should Be Part of Baseline Privacy Legislation**

Expanding the FTC’s security authority would be most effective upon passage of comprehensive federal privacy legislation. Unlike other developed countries, the U.S. currently lacks a comprehensive privacy law that would protect consumers across all sectors of the economy. The current patchwork of state laws does not provide the most effective protection for consumers. A baseline data privacy law would require companies to collect only as much personal information as necessary, be clear about with whom they’re sharing information, and expunge information after it is no longer needed.

<sup>41</sup> Adam Tanner, *Why You Should Use a Masked Credit Card to Shop Online*, Forbes (Dec. 4, 2013, 12:12 PM), <http://www.forbes.com/sites/adamtanner/2013/12/04/why-you-should-use-a-masked-credit-card-to-shop-online/>.

<sup>42</sup> Testimony of Justin Brookman, Center for Democracy & Technology, United States House of Representatives Committee of Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade (May 4, 2011), available at [https://www.cdt.org/files/pdfs/20110504\\_bonomack\\_jb.pdf](https://www.cdt.org/files/pdfs/20110504_bonomack_jb.pdf).

The Fair Information Practice Principles (FIPPs) must be the foundation of any comprehensive privacy framework. FIPPs have been embodied to varying degrees in the Privacy Act, Fair Credit Reporting Act, and other sectoral federal privacy laws that govern commercial uses of information online and offline. The formulation of the FIPPs by the Department of Homeland Security<sup>43</sup> and the more recent formulation adopted by the Administration in its Consumer Privacy Bill of Rights<sup>44</sup> offer a robust set of modernized principles that should serve as the foundation for any discussion of consumer privacy legislation. Those principles are:

- Transparency
- Purpose Specification
- Use Limitation
- Data Minimization
- Data Accuracy
- Individual Participation
- Security
- Accountability

Although data security, individual access to personal information, and notification of breaches are important safeguards under the FIPPs, it is crucial that baseline consumer privacy legislation not give short shrift to the other FIPPs, such as data minimization. Companies should collect only that data which is directly relevant and necessary to accomplish a specified purpose, and data should only be retained for as long as is necessary to fulfill a specified purpose. Unlike breach notification, data minimization is a pre-breach remedy and should be an obligation of all companies that collect personal information. Requiring companies to delete unneeded consumer data would reduce the impact of data breaches, and potentially result in fewer targets for identity thieves. We believe that requiring reasonable data minimization would result in less consumer information being exposed through data security breaches.

Comprehensive privacy legislation should also provide consumers with reasonable access to the information that companies possess about them. When companies collect, maintain, and transfer personal data to third parties, enabling individual consumers to access their personal data files and point out possible errors can provide an important safeguard against inaccuracy and misuse, and also provide needed transparency to consumers about the wide range of entities that possess and use information about them.

As data flows have grown more complex, companies must have safeguards in place to monitor them. The fact that major data breaches continue to occur demonstrates that current practices

<sup>43</sup> U.S. Department of Homeland Security, Privacy Policy Guidance Memorandum, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security, December 2008, [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_policyguide\\_2008-01.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf).

<sup>44</sup> WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), available at <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

for collecting and storing consumer data have outstripped the practices for keeping it safe. The most effective solution will not lie in an isolated effort to apply encryption to data or to quickly notify consumers of a data breach, although both encryption and notification are important. Rather, the law should provide companies with a range of incentives and requirements that encourage them to establish internal policies that seamlessly protect data throughout the data's lifecycle. A comprehensive data protection framework coupled with strong enforcement is that solution. CDT looks forward to working with both chambers to enact strong privacy protections for American consumers.

## **VII. Conclusion**

CDT would like to thank the Committee for calling this hearing on such an important topic, and for the opportunity to testify today.

For more information, contact Justin Brookman, [justin@cdt.org](mailto:justin@cdt.org), at (202) 637-9800.



Justin Brookman is the Director for the Center for Democracy & Technology's (CDT) Project on Consumer Privacy. Mr. Brookman coordinates CDT's advocacy on corporate collection, use, and retention of personal information, including efforts to enact comprehensive privacy legislation in the United States and to strengthen privacy law in Europe. Mr. Brookman has testified before House and Senate Committees on location privacy and data security, as well as the general need for stronger consumer privacy protections. He also leads CDT's work on behavioral advertising and the development of a "Do Not Track" setting for web browsers, and serves as editor of the compliance specification in the World Wide Web Consortium (W3C) standardization process. Under Mr. Brookman's direction, CDT has filed formal complaints with the Federal Trade Commission against companies that violate users' privacy and free expression rights. He also runs the Internet Privacy Working Group, a diverse set of privacy stakeholders including industry participants and other advocates, to formulate best practices guidance and inform CDT's own views on emerging privacy issues.

Prior to joining CDT in January 2010, Mr. Brookman was Chief of the Internet Bureau of the New York Attorney General's office. Under his leadership, the Internet Bureau was one of the most active and aggressive law enforcement groups working on internet issues, and Mr. Brookman brought several groundbreaking cases to protect the rights of online consumers. He brought the first regulatory actions against spyware and adware companies, as well as against the advertisers who funded those companies. He also brought several privacy cases against companies who misused or misappropriated consumers' personal information, including the first enforcement of Gramm-Leach-Bliley's restrictions on the use of consumer financial data. In 2009, Mr. Brookman brought the first case against a company for "astroturfing" --- or seeding internet message boards and blogs with fake positive reviews. He also brought important actions to preserve free speech online and to preserve network neutrality.

Mr. Brookman previously worked as a litigation associate for six years at Fried, Frank, Harris, Shriver & Jacobson LLP in both its New York and Washington offices. He received his J.D. from the New York University School of Law in 1998 and his B.A. in Government and Foreign Affairs from the University of Virginia in 1995.

Chairman BROWN. Thank you, Mr. Brookman.

We are going to recess until after this vote series. Members, be aware that we are going to resume 10 minutes after the last vote begins, so please hurry back. My Democratic colleagues have agreed to that, so we will recess and be back.

Gentlemen, thank you for your patience, appreciate it.

[Recess]

Chairman BROWN. Okay. We will reconvene this hearing, and I appreciate all the witnesses' patience with us and particularly Mr. Chabinsky. I appreciate your patience. Maybe we saved the best for last, but anyway, I have always been very concerned about privacy issues and I know you are, too.

Mr. Chabinsky, you have five minutes.

**TESTIMONY OF MR. STEVEN CHABINSKY,  
SENIOR VICE PRESIDENT OF LEGAL AFFAIRS,  
CROWDSTRIKE, INC.;**

**FORMER DEPUTY ASSISTANT DIRECTOR,  
FEDERAL BUREAU OF INVESTIGATION—CYBER DIVISION**

Mr. CHABINSKY. Thank you. Good morning, Chairmen Broun and Bucshon, Ranking Members Maffei and Lipinski, and distinguished Members of the Subcommittees.

I am pleased to appear before you today to discuss the role of technology in protecting Americans from international cybercrime. I have spent over 15 years committed to reducing the security risks associated with emerging technologies. And the observations and conclusions I am sharing today in my individual capacity are the culmination of a career spent in government—mostly with the FBI—industry, and academia.

First, I would like to address the cyber threat landscape. Over the past 10 years, industry has faced a well-orchestrated hacking epidemic. Foreign intelligence services are siphoning off our intellectual property and weakening American competitiveness, while organized criminal groups steadily gain access to corporate and consumer credentials that have been used to defraud Americans out of billions of dollars.

On the nation-state side, China and Russia continue to engage in massive cyber economic espionage campaigns that impact thousands of corporate victims daily.

With respect to financially motivated cybercrime, a disproportionate amount of it appears to be tied to Eastern Europe. On the FBI's current cyber most wanted list, for example, 7 of the 10 individuals have connections either to Russia, Ukraine, or Latvia.

Next, I would like to discuss our failed cybersecurity strategy. We keep spending more and more money and the problem keeps getting worse. I propose this is because we are focusing on the wrong part of the solution. Faced with the choice of trying to make our systems impenetrable—also known as vulnerability mitigation—or trying instead or at least an equal part to dissuade people from hacking into our systems in the first place—which would be threat deterrence—we have focused our resources almost entirely on the former, vulnerability mitigation. Our failed strategy dramatically raises the costs to the victims without substantially raising the costs to the bad guys. In fact, our failed strategy has poten-

tial victims fearing for the loss of their data more than actual hackers are fearing for the loss of their freedom.

We spend without end on vulnerability mitigation, despite it being well-understood that completely securing networks is a daunting, impossible task even for the most experienced. There simply is no chance that industry can consistently withstand intrusion attempts from foreign intelligence services and global organized crime groups. As a result, improving our security posture requires that we reconsider rather than simply redouble the nature of our efforts.

Fundamentally, we need to ensure that our cybersecurity strategies, technologies, market incentives, and international dialogue focus greater attention on the challenges of more quickly detecting and mitigating harm while in parallel locating and penalizing bad actors. Doing so also would align our cybersecurity efforts with the security strategies we use in the physical world.

In the physical world, vulnerability mitigation efforts certainly have their place. We take reasonable precautions to lock our doors and windows, but we do not spend an endless amount of resources in hopes of becoming impervious to crime. Instead, to counter determined thieves, we ultimately concede that an adversary can gain unlawful entry, but through the use of burglar alarms and video cameras, we shift our focus towards instant detection, attribution, threat response, and recovery.

When the alarm monitoring company calls a business owner at 3:00 a.m., it does not say we just received an alarm that your front door was broken into, but don't worry, we have called the locksmith. Rather, it is only obvious, immediately necessary and the reason people purchase alarm systems, that they call the police to stop the felon.

It is surprising then and suggests a larger strategic problem that in the world of cyber, when the intrusion detection system goes off, the response has been to call the chief information security officer and perhaps even the CEO to explain what went wrong and to demand that they prevent it from happening again.

In answer to the question of this hearing, technology can play a vital role in protecting Americans from international cybercrime, but to achieve that result, technology must be used in greater part to achieve threat deterrence. In that way, businesses and consumers will benefit from improved, sustained cybersecurity and will enjoy those benefits at lower costs.

Thank you for the opportunity to testify today. I would be happy to answer any questions you may have.

[The prepared statement of Mr. Chabinsky follows:]

Testimony of

Steven R. Chabinsky

Jointly before the  
United States House of Representatives  
Committee on Science, Space, and Technology

Subcommittee on Oversight  
and  
Subcommittee on Research and Technology

*"Can Technology Protect Americans from  
International Cybercriminals?"*

March 4, 2014

### **Introduction**

Good morning Chairmen Broun and Bucshon, Ranking Members Maffei and Lipinski, and distinguished Members of the Subcommittees. I am pleased to appear before you today to discuss the role of technology in protecting Americans from international cybercrime. Within this context, I have been asked to provide an overview of the evolution of cyber intrusions against U.S. industry -- from rogue hackers, to sophisticated international crime syndicates, and to foreign governments. I also have been asked to describe the complex cyber security issues facing industry and how the risk of cyber threats and intrusions can best be managed.

### **Background**

I have spent over fifteen years committed to reducing the security risks associated with emerging technologies. Most of my efforts have been with the Federal Bureau of Investigation, where I last served as Deputy Assistant Director of the Cyber Division, after having organized and led the FBI's cyber intelligence program and served as the FBI's top cyber lawyer. Today, I am the General Counsel and Chief Risk Officer of the cybersecurity technology firm CrowdStrike, as well as an adjunct faculty member of George Washington University and the cyber columnist for *Security* magazine. The observations and conclusions I am sharing today in my individual capacity are the culmination of a career spent in government, industry, and academia.

### **The Evolution of Computer Intrusions**

As is the case with more traditional threats, we see a wide range of actors who are capable of, and engaged in, computer network intrusions and attack. Although rogue hackers have the ability to cause substantial harm against specific targets (especially when they are insiders), the far greater problem is that most hackers no longer work alone. Rather, over the past ten years, industry has faced a well-orchestrated hacking epidemic. Foreign intelligence services are siphoning off our intellectual property and weakening American competitiveness, while organized criminal groups steadily gain access to corporate and consumer credentials that have been used to defraud Americans out of billions of dollars.

On the nation-state side, China and Russia continue to conduct massive economic espionage hacking campaigns that impact thousands of corporate victims daily, not just in the United States but worldwide. As expressed in May 2013 by the Commission on the Theft of American Intellectual Property, the impact on victim economies are twofold. The first harm takes the form of lost revenues and lost jobs. The second harm is the erosion of "both the means and the incentive for entrepreneurs to innovate, which will slow the development of new inventions and industries."

Switching our focus to financially motivated cybercrime, we can break down the most common activities into two broad categories. First, there are traditional forms of fraud that now occur using email rather than regular mail, like the infamous Nigerian Letter scam. These schemes rely on social engineering, but they do not involve unauthorized computer access. Second, there are the more pernicious cybercrimes that seek to install malware on victim computers in order to control their processes and/or steal their data from afar. Hackers have a variety of techniques for installing malware on computers. They may rely upon phishing emails with links or attachments, supply chain infections, or compromised websites. Others may engage in remote computer intrusions that exploit software weakness, or take advantage of an ability to obtain, guess, create, or bypass legitimate user credentials. Regardless, cybercriminals in this second category typically gain access to a large number of victim networks, and obtain the ability to see and do most anything on them.

A few years ago, the FBI identified ten specializations within a typical cyber conspiracy. It is worth repeating them here to demonstrate the extent of capabilities available in the world of organized cybercrime. First, there are “coders” who write the malware, exploits, and other tools necessary to commit the crime. Second, there are “distributors” who trade and sell stolen data. Third, are the “techies” who maintain the criminal infrastructure. Fourth are the actual “hackers” who search for and exploit application, system, and network vulnerabilities. Fifth, there are “fraudsters” who create and deploy social engineering schemes, including phishing, spamming, and domain squatting in order to gain unlawful access. Sixth are “hosters” who provide “safe” hosting of illicit content servers and sites, often through elaborate botnets and proxy networks. These individuals specialize in the area of anonymization, setting up elaborate network infrastructures with encrypted servers running on networks that, by design to cater to criminals, do not log user activity and do not shut down websites regardless of complaints of unlawful conduct. Seventh are “cashers” who control drop accounts for money. Eighth are “money mules,” some of whom are sent to the U.S. on student visas with the purpose of moving money for criminals. Ninth, are “tellers” who help transfer and launder illicit proceeds through digital currency services and between different world currencies. And finally, tenth are the “leaders,” many of whom don’t have any technical skills at all. They choose the targets, choose the people they want to work each role, decide who does what, when, and where, and take care of personnel and payment issues. With respect to planning and logistics, when a new opportunity presents itself, these criminal organizations often start executing within hours.

### **The Location of Cybercrime**

Over the years, it appears that a disproportionate amount of financially motivated cybercrime is tied to Eastern Europe. Of the FBI’s current Top Ten Cyber Most Wanted, seven have connections either to Russia, Ukraine, or Latvia. In some cases, international cybercriminals are suspected of receiving the protection of local authorities. Regardless, even to the extent cybercrime ringleaders may aggregate in

certain areas of Europe, they typically are part of criminal conspiracies that span the globe.

For these reasons, it is imperative that law enforcement agencies throughout the world build strong relationships with one another and resource the capabilities that are necessary to quickly work together in common cause, whether to collect evidence, to recover stolen property, or to bring criminals to justice. One cannot overstate the importance of programs like the overseas FBI Legal Attaché assignments. The FBI testified last June that it had embedded cyber agents with law enforcement in several key countries, including Estonia, Ukraine, the Netherlands, Romania, and Latvia, and that it was expanding its Cyber Assistant Legal Attaché program to the United Kingdom, Singapore, Bulgaria, Australia, Canada, the Republic of Korea, and Germany. These efforts, together with complementary actions taken by the United States Secret Service, are designed to decrease the number of hackers worldwide (whether through arrests or based on their threat deterrent effect), and are likely to demonstrate consistent benefits over time that far outweigh their costs. These efforts also help fulfill a primary role of government to protect its citizens and their property.

#### **The Victims of Cybercrime and Cyber Economic Espionage**

Next, it is important to consider the victims associated with cybercrime, and to recognize that many of them do not have the resources to mount a significantly stronger defense than they currently are against computer attacks. It certainly is the case that the cyber intrusion headlines tend to focus on the Fortune 100 being hacked; but they're not the only victims. Naturally, since 99.9% of all U.S. businesses have less than 500 employees, and few of those retain dedicated information security staff, cyber criminals find small and medium enterprises (SMEs) to be attractive targets as well. Making matters worse, targeted attacks against SMEs appear to be increasing.

#### **Core Tenets of Security**

In order to get security risks under control, whether in the "physical" or cyber worlds, security experts rely upon the levers of vulnerability mitigation, threat reduction and, should the first two fail, consequence management. In the area of cybersecurity, vulnerability mitigation has been our nation's predominant approach. Unfortunately, the majority of our government and private sector resources focus on having potential victims fear for the loss of their data, rather than having actual hackers fear for the loss of their freedom.

We have retained this focus on vulnerability mitigation despite it being well understood that securing networks is a daunting task even for the most experienced. As stated in Verizon's 2013 Data Breach Investigations Report, "breaches are a multi-faceted problem, and any one-dimensional attempt to describe them fails to adequately capture their complexity." On the technical side—the web servers, e-mail

servers, databases, firewalls, routers, embedded network devices, internal networks, global remote access, custom applications, off-the-shelf applications, backup and storage areas, and all telephone, PBX, and VoIP systems require attention. On the human side, the physical infrastructure must be protected, employee accesses and permissions must be restricted, and connections to business and corporate partners (often operating under different legal regimes) have to be managed. Of course, these are just the basics, and each aspect of cybersecurity must be monitored and updated regularly, as the technologies, users, and adversaries change constantly.

In order to reduce the likelihood of harm, information security professionals deploy a wide range of defensive controls. In answer to the question posed by this Hearing, one of those controls most certainly involves the use of technology. In the risk management community these are commonly referred to as *technical* controls. Examples of technical controls include the use of smart cards with encryption, passwords and biometrics, endpoint activity monitoring, firewalls, and intrusion detection and prevention systems. In my professional opinion, technical controls (not “people,” as often is said) are best positioned to be a company’s first line of cyber defense. Technical controls are particularly well suited to reduce the time necessary to detect unlawful activity and to substantially limit the consequences of a successful breach. Still, although technical controls often are necessary for security, they are seldom sufficient. Security professionals also commonly deploy *physical* controls (such as locks on doors) and *administrative* controls (such as acceptable computer use policies and pre-employment background checks). Each of these controls, deployed together as a “defense in depth,” serves to protect industry from cybercrime.

To get a better feel for the difficulties of being a cybersecurity professional, it is worthwhile to consider, at the 30,000 foot level, the following seventeen different categories that NIST recommends network defenders review (keeping in mind that each of these is then broken down further into more discrete, tactical methods):

1. access control;
2. awareness and training;
3. audit and accountability;
4. certification, accreditation, and security assessments;
5. configuration management;
6. contingency planning;
7. identification and authentication;
8. incident response;
9. maintenance;
10. media protection;
11. physical and environmental protection;
12. planning;
13. personnel security;
14. risk assessment;
15. systems and services acquisition;
16. system and communications protection; and

### 17. system and information integrity.

Continuously reviewing and implementing the technical, physical, and administrative controls within each of these seventeen categories can help prevent some aspects of international cybercrime altogether and, in the event of a successful breach, can quickly detect the intrusion and mitigate the consequences. However, relying upon the owners and operators of networks to be primarily responsible for stopping well-resourced, determined actors – without a similar or greater alignment of government resources to bring international offenders routinely to justice -- has turned out to be exorbitantly expensive and ineffective over time.

In this regard, it is also worth noting that hackers usually take advantage of the easiest path to exploit a system. For this reason, it often is difficult to anticipate the long-term impact of industry best practices and costly mitigation efforts: will the hackers be foiled, seek a different victim, pull something else out from their existing criminal toolkit, or devise a new exploit? I am reminded of costly efforts that the banking and finance sector adopted a few years back, providing business customers with key fobs in which the pin numbers changed every sixty seconds. The bad guys simply redirected the pin numbers to themselves the moment the customers entered them into their infected web browsers. To similar effect, I also recall Intellectual Property Rights investigations that uncovered thieves who invested tens of thousands of dollars to buy machines that added hologram stamps to their counterfeit software CDs and DVDs. I have also observed that bad guys tend not to get discouraged by minor setbacks, and they will continue their unlawful activities unless they get caught or believe they will get caught. After all, cybercrime is big business, and the bad guys have time to seek out new vulnerabilities and explore new techniques. In the context of today's discussion about crimes against the retail industry, we cannot forget recent experiences in the United Kingdom where, after spending in excess of one billion dollars on new technologies, one media headline read, "Card fraud hits record high despite fortune spent on chip-and-pin security." A professor at Cambridge University then lamented, "It has simply led to a change in [criminal] tactics."

### Conclusion

There is no doubt that cyber threats present considerable risk to our economic and national security interests, and that these threats continue to grow at an alarming rate. Despite billions of dollars of investment in cybersecurity defensive efforts, and the prospect of spending billions of dollars more, many experts see no hope on the horizon that the overall cyber threat against our country will level off, no less begin to decline. It is my professional opinion that this downward spiral is not inevitable and that we can improve our security considerably. However, it also is my professional opinion that improving our security posture requires that to a certain extent we reconsider, rather than simply redouble, the nature of our efforts.

Fundamentally, we need to ensure that our cybersecurity strategies, technologies, market incentives, and international dialogue focus greater attention on the

challenges of more quickly detecting and mitigating harm, while in parallel locating and penalizing bad actors. Doing so would align our cybersecurity efforts with the security strategies we use in the physical world. In the physical world, vulnerability mitigation efforts certainly have their place. We take reasonable precautions to lock our doors and windows, but we do not spend an endless amount of resources in hopes of becoming impervious to crime. Instead, to counter determined thieves, we ultimately concede that an adversary can gain unlawful entry but, through the use of burglar alarms and video cameras, we shift our focus towards instant detection, attribution, threat response, and recovery. When the alarm monitoring company calls a business owner at 3 a.m., it does not say, "We just received an alarm that your front door was broken into. But, don't worry, we've called the locksmith." Rather, it is only obvious, immediately necessary, and the reason people purchase alarm systems, that they call the police to stop the felon. It is surprising then and suggests a larger problem that, in the world of cyber, when the intrusion detection system goes off the response has been to call the Chief Information Security Officer, and perhaps even the CEO, to explain what went wrong and to prevent it from happening again. It is my hope for the future that the blame for, and the costs of, cybercrime will fall more squarely on the offenders than on the victims, that in doing so we will achieve greater threat deterrence, and that businesses and consumers will benefit from improved, sustained cybersecurity at lower costs.

Thank you for the opportunity to testify today. I would be happy to answer any questions you may have.

**Steven R. Chabinsky**

Steven Chabinsky is Senior Vice President of Legal Affairs, General Counsel, and Chief Risk Officer for CrowdStrike, a big data cybersecurity technology firm that specializes in continuous threat detection, cyber intelligence, and computer incident response. Steve also serves as an adjunct faculty member of George Washington University, and as the cyber columnist for *Security* magazine. Before joining CrowdStrike,

Mr. Chabinsky had a distinguished 17-year career with the government, culminating in his service as Deputy Assistant Director of the FBI's Cyber Division. Prior to that role, Mr. Chabinsky organized and led the FBI's cyber intelligence program, and was the FBI's top cyber lawyer. Mr. Chabinsky also served in the Office of the Director of National Intelligence (ODNI), where he rose to become Acting Assistant Deputy Director of National Intelligence for Cyber, Chairman of the National Cyber Study Group, and Director of the Joint Interagency Cyber Task Force.

A graduate of Duke University and Duke School of Law, Mr. Chabinsky began his legal career as an associate with Simpson Thacher & Bartlett in New York, and as a law clerk for the Honorable Dennis Jacobs of the United States Court of Appeals for the Second Circuit. Mr. Chabinsky is the recipient of numerous awards and recognitions, including the National Intelligence Distinguished Service Medal. In 2012, he was named one of *Security* magazine's "Most Influential People in Security."

Chairman BROUN. Thank you, Mr. Chabinsky.

I want to thank the witnesses for your testimony, now reminding Members that Committee rules limit questioning to five minutes. The Chair will open the first round of questions. The Chair recognizes himself for five minutes.

I ask this of all five of you. What is the fastest and the best way to get new innovations deployed to protect the safety, privacy, and security of consumers' financial data? Government mandates that pick technological winners and losers or allowing maximum competition for customers in the market by companies offering innovative security solutions and consumer protections against new, evolving, and changing threats that go way beyond the requirements of a static law?

Start with Mr. Romine.

Dr. ROMINE. Thank you, Mr. Chairman. I think it is clear that in order to maintain the kind of innovation that is needed on the defensive side for us to protect our assets and our networks, we have to be just as agile as the innovation that is taking place with our malefactors. And so, I think having additional regulation is probably not the answer from our perspective. We have a voluntary program associated, for example, as I talked to earlier in my testimony about the cybersecurity framework for critical infrastructures that NIST worked on, and that is a purely voluntary program in part because we believe that that enables the private sector to maintain an innovative approach to the kind of defenses that are needed.

Chairman BROUN. Very good. Mr. Russo?

Mr. RUSSO. Thank you for the question. I think the PCI Security Standards Council is uniquely qualified to do exactly what you are looking for. We have a network of over 1,000 merchants, banks, vendors, associations worldwide that submit feedback to us on a regular basis indicating what they are seeing in their region and then their particular verticals, and all of this is factored into creating the absolute best defenses that we can to protect this data. Right now, I think that the best defense against a breach are the PCI standards.

Chairman BROUN. Very good. Mr. Vanderhoof?

Mr. VANDERHOOF. Yes, thank you. There really needs to be multiple layers of security around payments data, so certainly we need to devalue the data that currently exists in this system, and there are alternative technologies using chip technology, as well as other techniques such as tokenization that are being developed to try to accomplish that goal.

Also, we certainly need to continue to strengthen the networks that are using this data and the efforts that have been made by the PCI Council and by other cybersecurity best practices are going a long way towards doing that. And I think we need to also maintain and invoke strong enforcement of when data breaches do occur in terms of trying to track down the people responsible for that and preventing future breaches from happening.

Chairman BROUN. Mr. Brookman.

Mr. BROOKMAN. Yes. So I certainly don't think that legislatively prescribing technological solutions is a good idea. However, I think it would be a good idea to maybe strengthen the Federal Trade

Commission's authority to go after bad data security practices. Right now, that authority is somewhat unclear, and even when they do bring those cases, they don't have the ability to get penalties for bad practices.

So I think strengthening them, creating more incentives for companies and for banks and for merchants to deploy better technological solutions is probably the best approach.

Chairman BROWN. Mr. Chabinsky?

Mr. CHABINSKY. Thank you, Mr. Chairman.

I think fundamentally we need a bit more research and development in the area of return on investment. It is very difficult for us to understand whether the value of security that is being proposed in the marketplace will have a commensurate benefit as to the cost. We have heard a lot within this hearing as well as prior ones about the costs of implementing certain solutions, in certain cases mounting into the billions of dollars. And it is very difficult for industry to understand whether or not that is a benefit that outweighs the cost that we are seeing. So I would suggest that this Committee is in a good position to explore government research that would spend more time looking at the metrics of success and the return on investment.

Chairman BROWN. Okay. Thank you, Mr. Chabinsky.

Mr. CHABINSKY. Thank you.

Chairman BROWN. I have a question for all of you. As a physician, I am very concerned particularly with the question about protection of privacy and security in the healthcare industry and the insurance industry. I have half a minute left. Does anybody want to take on what we can do to protect privacy in patient records and that sort of thing?

Mr. Vanderhoof.

Mr. VANDERHOOF. Yes, thank you, Chairman.

I think the problem we have with the imposed changes that are happening in the healthcare system around the use of electronic data for health records is that we have failed to be able to authenticate who are the actual individuals that have authorized access to that data and be able to positively identify the individual that owns that data so that when health information is being digitized and being used and shared across different professional entities, there needs to be a way to protect the access to that information and so that that information can't be then stolen and be used for other purposes. And having this ability to strengthen the health IT system in similar ways is really another way forward to making sure that consumer health information stays protected.

Chairman BROWN. Thank you, Mr. Vanderhoof.

My time is expired, but I would like for all five of you to answer that question for the record in written form.

And, as a physician, I am very concerned about a central repository of all health records. I think there should be a better way so that patients control their own electronic medical records and not the Federal Government and not an insurance agent or the insurance industry. And so I would appreciate any input from all of you.

My time is expired. Mr. Maffei, you are recognized for five minutes.

Mr. MAFFEI. Thank you, Mr. Chairman.

I guess I will start with Dr. Romine. Where are these threats and incursions coming from generally? I mean where are the criminals, if you will, coming from?

Dr. ROMINE. So I think there are a number of places, and I think Mr. Chabinsky is absolutely right. Some of them are intelligence services from other governments seeking our intellectual property for their competitive advantage. Some of them are organized crime, highly organized and capable, and those are international as well. So I think, Mr. Chabinsky is accurate on that score.

Mr. MAFFEI. Mr. Russo, you and I talked about this a little bit. Do you have an idea of how many are external to the United States? Is there any way to trace that or figure that out?

Mr. RUSSO. There probably isn't a good way to trace that. Obviously, some of the major breaches that we are seeing now are being perpetrated from outside the United States. As a matter of fact, I picked up a USA Today this morning and there was a big article about this malware coming from someplace outside of the United States as well.

I would agree with Mr. Chabinsky. I think one of the areas that we would like to see a little more help in is bringing some of these people to justice, stiffer fines, and the ability to stop this thing. We are basically in an arms race when it comes to security, and while we are staying up with them and staying ahead in some cases, you need to be vigilant all the time. And unfortunately, many businesses are not vigilant 365, 24/7, and hackers need to be vigilant one day.

Mr. MAFFEI. Right. Exactly.

Mr. Chabinsky, do you have any—I—DD is—are there any estimates about how many threats are from outside the United States? And also if you have a related comment.

Mr. CHABINSKY. I don't—I am not aware of any actual estimates but I think it is only natural that hackers being able to remotely gain access are less likely to hit domestically where they are. Right? So you would see that other nations are experiencing hacking that would include hacking from the United States and that we are more likely to then have hacking from abroad.

Certainly, there is no doubt that a lot of the financial fraud that we are seeing tends to be led or have strong ties to Eastern Europe. But equally true, those groups even that have those ties to Eastern Europe are global in nature and we have seen groups that are operating in dozens of countries simultaneously, hitting hundreds of cities at once. We saw one ring that was able to hit ATMs throughout the world in a 24-hour period and steal in excess of \$9 million within 24 hours on the ground. This turned out to be a proof of concept. A group later did it, stealing \$45 million. So it is certainly global.

I would say in that regard that law enforcement is well aware of that and the FBI for its part has a legal attaché program that they are using in no small part to help protect Americans against cyber threats. They have embedded agents not only within the embassies there but there are a number of nation-states that have invited our own law enforcement to sit side-by-side with them in their national Federal law enforcement agencies just to combat cyber. In that regard, the FBI has cyber agents sitting side-by-side

with cyber agents of other countries in Estonia, Ukraine, the Netherlands, Romania, and Latvia. Those are very helpful models to build on this international aspect of cybercrime law enforcement.

Mr. MAFFEI. So most of the time other countries are cooperative with our efforts and we are with theirs?

Mr. CHABINSKY. That is absolutely correct.

Mr. MAFFEI. But are there some instances of state sponsorship that we know of, anybody on the panel?

Mr. CHABINSKY. There are. China and Russia are certainly the most heavily invested in state-sponsored espionage. The relationship between nation-state espionage and cybercrime is uncertain in most areas. There certainly is a lot of information indicating that there can be an unsteady alliance at times between nation-states and criminal enterprises either because at the lower level of law enforcement, not typically at the Federal level, there could be corruption of state and local law enforcement protection, and at the higher levels, there may be an uneasy alliance where criminals are actually helping the intelligence service for nation-state aims while on the side being able to get rich quick, if you will, on criminal activities for which the nation-state might look the other way.

Mr. MAFFEI. Do we know where the data breach at Target originated?

Mr. CHABINSKY. I am not prepared today to discuss that matter.

Mr. MAFFEI. Anybody else know or—Mr. Russo, do you have any idea? Okay.

Well, I would submit to the Committee that this is an important—I appreciate the Chairman—the two Chairmen for holding this hearing but that this is also a severe national security concern. And the fact that we don't even know how many of these threats are coming from outside the United States I just think, you know, makes it important to have additional scrutiny. So I will also be bringing it up in my other Committee, which is the Armed Services Committee, although that may not be the right one either, maybe Homeland Security. I am not sure.

But I really appreciate us drawing attention to it in this hearing.

Thank you, Mr. Chairman.

Chairman BROUN. Thank you, Mr. Maffei.

And I am on Homeland Security and we have looked into these issues and we will continue to do so.

Dr. Bucshon, you are recognized for five minutes.

Mr. BUCSHON. Thank you, Mr. Chairman.

On April 16 of last year, the House overwhelmingly passed two bipartisan Science Committee bills to assist the private sector and other domestic organizations to secure their information systems. Each bill got over 400 votes.

The first is H.R. 756, the Cybersecurity Enhancement Act, which requires a government-wide IT security R&D plan, authorizes the National Science Foundation basic research on cybersecurity with scholarships and support for cybersecurity education, human resource development, and directs NIST to coordinate Federal activities on international cybersecurity technical standards development.

The other bill is H.R. 967, the Networking and Information Technology R&D, or NITRD Act. It updates the NITRD program on cybersecurity and it focuses the NITRD program on R&D to detect, prevent, resist, respond to, and recover from actions that compromise or threaten to compromise the availability, integrity, or confidentiality of computer and network-based systems. Unfortunately, neither one of these bills have been taken up in the Senate and so right now they are kind of in limbo.

The question I have is to the entire panel. Would these bills help protect Americans from international cyber criminals? And maybe we should suggest that the Senate pass the bills if that is the case.

So I will start with Dr. Romine.

Dr. ROMINE. Thank you. There are many provisions of these bills that are very constructive in addressing the very complex issue of cybersecurity, and NIST has had a very close working relationship in collaboration or discussions with the entire Committee and your Subcommittee and your staff and we look forward to continuing to engage on that.

Mr. RUSSO. Thank you, Congressman. The Council does not endorse or comment on any specific legislation, but these bills certainly represent concepts that we support.

Mr. VANDERHOOF. Yes, and likewise, the Smart Card Alliance does not advocate on behalf of any specific legislation. However, in principle, we certainly do believe that more research can be done to help stimulate private industry in terms of looking for creative solutions to try to fight cybercrime.

Mr. BROOKMAN. My office does take positions on legislation. We have not taken positions on these two bills. I think there are some really good things in there that are incredibly important and would be productive. My only caveat would be I would want to ensure that additional funding and research was given to NIST to fulfill the requirements that they would do under those bills and not take away from existing resources.

Mr. CHABINSKY. Chairman Bucshon, I fully support the goals of both bills. I believe that in order to protect our economic and national security, including better protecting Americans from international cybercrime, the Federal Government must increase its investment in research and development, as well as in cyber workforce development.

I would respectfully recommend only that this Committee keep an eye on how government-supported R&D resources are allocated, keeping in mind that the best long-term strategy for protecting Americans from criminals, whether they are near or far, is in my opinion not through enhanced defenses but rather through better detection of, attribution of, and penalties against the criminals themselves.

These bills can promote the goals of enhancing cyber threat deterrence, and I am grateful for the attention of the Committee in advancing them.

Mr. BUCSHON. Thank you very much. I want to make one comment. I think on this whole issue that the American public is very acutely aware of the privacy issues related to cybersecurity but not as aware of—in my opinion when I talk to people—of what the threats and the risk to breaches in cybersecurity are because of the

attention brought by the national media leaning more towards the privacy issue, which is an extremely important issue of course.

But I think all of us could in some way be helpful by exposing more of what the risk actually is other than just losing your credit card data, which is very important of course, but a bigger issue is, for example, if half of America all of a sudden loses power suddenly or the entire country loses power or our GPS system shuts down, what the risk of that is.

Mr. Romine and Mr. Russo, is the private sector capable of successfully developing and following security standard for itself or does it need government assistance or oversight?

Dr. ROMINE. So in this case, the NIST position is clear that in the development of the cybersecurity framework we worked very closely and collaboratively with the private sector and we believe that those voluntary approaches are in fact going to be very effective.

I would say government assistance, however, in the sense that NIST has been acting as a convener for those discussions, is very helpful.

Mr. BUCSHON. Mr. Russo, quickly, because my time is up.

Mr. RUSSO. I would agree. The standards are adaptable. They are developed in collaboration with a huge amount of input globally, so I think we are uniquely qualified to handle specifically payment card data.

Mr. BUCSHON. Thank you very much. I yield back, Mr. Chairman.

Chairman BROWN. Thank you, Dr. Bucshon.

My friend Dan Lipinski, you are recognized for five minutes.

Mr. LIPINSKI. Thank you, Mr. Chairman. I want to thank Chairman Bucshon for talking about those two bills. You saved me a little bit of time. I want to especially mention the Cybersecurity Enhancement Act, which is the bill that I have done with Congressman McCaul. In past Congresses also, and as often happens, we are waiting for the Senate to act. Hopefully, they will move soon on that.

So that moves me into my next question, which is for Mr. Brookman and Mr. Romine, but anyone else can jump in.

Technology plays an important role in countering cyber threats, but we all know that there are important other factors that can contribute to cyber attacks also. Human factors often help facilitate successful cyber intrusions by individuals who mistakenly or incorrectly give up passwords or open up emails from strangers, for instance, or they make their password "password," as was mentioned earlier.

From a cybersecurity and cyber policy perspective, how do we begin to address those elements to help counter cyber attacks? That is, what is the importance of social science research especially to look at the problems of cybersecurity that come from human factors, and what can be done to encourage people to practice better cyber hygiene?

So let's start with Mr. Brookman.

Mr. BROOKMAN. Sure. So I am not a researcher but I know there is a lot of good social science research going on on these issues. I know Carnegie Mellon University, for example, Dr. Lorrie Cranor,

also UC Berkeley has done some really good work with Chris Hoofnagle, Stanford, Alicia McDonald, did a lot of looking into these issues about what kind of nudges you can give to folks to do the right thing. I don't know how much their research has been implemented in the marketplace.

From a policy perspective, I think the most important thing you can do is to put the incentives in place to make companies make the right decision that if they have a liability, they are the ones who have to push people to do harder passwords. I think it is very hard to prescribe that at a Federal level, but I think, you know, putting stronger incentives on companies to—in the event that they let people do passwords, then perhaps their liability I think is probably the best solution.

Mr. LIPINSKI. All right. Dr. Romine?

Dr. ROMINE. Thank you. I am pleased to be able to say that my laboratory has an active research program in the usability of security. We have staff of psychologists, human factors, engineers, computer scientists that are working on this problem.

And I would like to make a couple of points. One is, of course, regulating behavior is often not going to be as effective as making strides in usability. The goal is to make it easy to do the right thing, make it hard to do the wrong thing, and make it easy to recover when the wrong thing happens anyway.

And the other thing I would say is this idea that there is a trade-off between usability and security is a false dichotomy. The fact is that you can actually achieve better security, more realized security if you improve the usability of the security and particularly the identity management that you are undertaking.

Mr. LIPINSKI. Does anyone else want to comment on that at all?

Let me move on then to the notification of these cyber breaches. There is currently no Federal data breach notification regulation. For many cyber tests, consumers are not notified for days or longer after a company realizes it has been successfully attacked. And Mr. Chabinsky had talked about what usually is the—what the response is. Can each of you give us very briefly your thoughts on requiring a national data breach notification requirement? Let's start with Mr. Chabinsky and go across.

Mr. CHABINSKY. I fully support the goals of a national data breach law. Right now, industry is subjected to I think at last count it is 46 different data breach statutes on the books across our land. That is making it very difficult not only for consumers to get any sort of consistent approach in data breach notification but for industry to actually have the confidence and ability to react in a quick way across so many different jurisdictions.

Mr. BROOKMAN. Yes. We are really ambivalent on the need for a Federal data breach notification. As you said, there are 46 States, so it is by and large already required. Making it more seamless, easier to have a data breach notification is arguably somewhat counterproductive, right? If it is easier for you to comply, well, then there is less incentive for you to get security right in the first place. So we think in order to be effective, you have to pair it with something else, some sort of comprehensive privacy or security requirements to make that effective for consumers.

Mr. VANDERHOOF. Yes, I definitely support some uniform data breach notification guidelines for industry rather than having a state-by-state approach because it does provide industry with a better framework by which they can set up their procedures to be able to uniformly inform their customers when a breach occurs.

I would only caution that notifying customers when a breach occurs and then notifying them what their risks are and what they are able to do to address those risks is still going to be up to the individual organization that has been breached, and therefore, there still needs to be control within the individual organization in terms of how they manage the relationship with their customers.

Mr. RUSSO. Congressman, as I indicated, the Council does not speak on legislation, but generally, we support awareness of these types of issues.

Mr. LIPINSKI. Thank you. Dr. Romine?

Dr. ROMINE. And I would agree that a further discussion needs to take place on whether that is an advisable approach. From my perspective as a NIST representative, it is outside the technical scope of our activities.

Mr. LIPINSKI. All right. Thank you very much. I yield back.

Chairman BROWN. Thank you, Dan.

Mr. Kilmer, you are recognized for five minutes.

Mr. KILMER. Thank you, Mr. Chairman.

I was going to start with Mr. Chabinsky. I am a member of the Armed Services Committee. In fact, I just came from there so apologies for being late. I know the military doesn't defend itself from cyber attacks by software alone. You know, they use a system of personnel training and physical security and IT to guard against would-be attackers. Does industry follow that approach, and if not, what percentage of risk would be—would investments in enhanced IT hardware and software cover?

Mr. CHABINSKY. Thank you for the question, Congressman Kilmer.

Industry does absolutely follow the same approach. That approach is in fact developed by NIST and adopted under FISMA. Basically, you are talking about three different controls that are put into place under a risk framework. There are technical controls and much of what the focus of this Committee is on the technology, and then we have already heard about the administrative controls, about trying to work with our personnel to ensure effective enforcement of our policies, and then physical controls, making sure people don't actually have access to our servers.

Those are exactly the same types of controls that are adopted in private sector standards that are international as well and that have been rolled out again in an actually quite elegant form in the cybersecurity framework.

I would, of course, note that the military systems themselves have been breached on numerous occasions and have not been able to withstand the onslaught of intelligence services, nor have the private sector. So I think everybody is working in a situation in which they are doing the best that they can following similar standards, but again, we are talking about an area where risk is controlled but there remains an unfortunately large amount of residual risk in this area.

Mr. KILMER. I am going to touch on something that there has been some discussion around already. I was a few months back in a meeting with a number of folks in the IT space and we were talking about cybersecurity issues, and the conversation found its way to how companies implement protection, invest in new software, and adopt best practices on avoiding cyber attack. And one of the folks in the room said, you know, governments—it is not the government's role to force compliance or force protection. And I asked the question, you know, can government in some way incent good cyber hygiene and incent compliance? Do you think government as it stands right now provides any incentive to industry to take steps it should to protect itself? And if so, how? And if not, what might that look like?

Dr. ROMINE. So speaking again from the perspective of the development of the cybersecurity framework that was just released last month, there have been discussions in place with regard to DHS helping with the voluntary program and they have rolled out something that they call now C3, which is their approach to providing assistance in using the framework. But there has always been, in addition to that, discussions about incentives that could be provided from the government, and those discussions would be productive going forward as well.

Mr. KILMER. Anything specific? I mean, go ahead, Mr. Vanderhoof.

Mr. VANDERHOOF. Thank you, Mr. Kilmer. So you mentioned the Department of Defense, which still today is pretty much the gold standard in terms of protecting its networks and cybersecurity effects. And what they did was they invested in their identity credentials to make those authentication technologies as strong as they possibly can so that they know who is allowed to be within their network to help prevent those people that are not allowed to be in the network from getting in the network.

And the government has adopted this common standard across the entire Federal enterprise using secure chip technology and have actually extended that technology standard that was set by NIST to the commercial entities that also do business with government.

So what has proven to be very effective on the commercial side has been government leading by example of protecting itself first, extending that level of standard for protection for commercial entities doing business with the government, and then that in turn has stimulated investment in those technologies that are then translated into the commercial spaces well.

Mr. BROOKMAN. I will say that for financial data I think the law does provide some pretty strong incentives. Data breach notification is incredibly painful and expensive. The PCI rules I think put pretty strong incentives there. For other categories of consumer data, though, I think they are actually very poor, including a lot of health data, right? To the extent health data is not governed by HIPAA and HITECH, to the extent you give information to an app or to some online service, there are very little protections at all security-wise.

The Federal Trade Commission has tried to be aggressive with its consumer protection authority, but even when they win, they

can't get any money. They just say, okay, promise to use better security in the future. So I think there should be stronger protections for other categories of consumer data.

Mr. CHABINSKY. On the incentive side, Department of Homeland Security is doing good work right now with the insurance industry to determine whether or not corporations will be able to find a better market in insurance to be able to transfer risk, and the insurance industry as a result is trying to think of ways that improved security will result in a market that will be both cost-effective and beneficial. So I think that that is one area that the government is working right now on the incentives side.

Of course in a national data breach notification law, should one exist, there is the potential to have certain safe harbors if certain encryption methodologies were in place or otherwise. So, I think that there are a number of incentives.

Again, my only caution is using any comparison between the private sector and the government with respect to data security and network security to have a more realistic discussion about the number of breaches that actually are actively being incurred against government systems with a lot of resources being put against them and mandates no less, not voluntary, and yet there still obviously are a lot of issues there.

Thank you.

Mr. KILMER. Thank you. Thank you, Mr. Chairman.

Chairman BROUN. The gentleman's time is expired.

I want to thank the witnesses for you all's valuable testimony. I am southern. Y'all is plural for you all. But I want to thank you all for you all's valuable testimony, and I really want to thank you for your flexibility and for your patience. I know you have been just kind of jerked around a little bit by the weather and changing schedules and vote series and you all have been extremely patient and extremely flexible with us. It has been a great hearing I think. All the Members, I am sure, have garnered a tremendous amount of information from you all and we appreciate you all considering getting back to us.

I want to remind Members that you all have a short period of time to get questions to them. In fact, in two weeks, we will submit questions for you all to answer. We call them questions for the record and they will be put in the record, and we appreciate your help on that.

So I do remind Members that if you have any additional comments or any additional questions to please get them in expeditiously.

Thank you all. You all are excused. This hearing is now adjourned.

[Whereupon, at 11:57 a.m., the Subcommittees were adjourned.]

## Appendix I

---

### ANSWERS TO POST-HEARING QUESTIONS

ANSWERS TO POST-HEARING QUESTIONS

*Responses by Dr. Charles H. Romine*

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY  
SUBCOMMITTEE ON OVERSIGHT  
AND

SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

**“Can Technology Protect Americans from International Cybercriminals?”**

**QUESTIONS FOR THE RECORD**

**Dr. Charles H. Romine**

**Director, Information Technology Laboratory, National Institute of Standards and Technology**

**Questions submitted by Chairman Broun and Chairman Bucshon**

1. What can be done to help banks, payment companies and merchants better collaborate on industry standards and innovative solutions to data breaches and cybercrime for electronic financial transactions?

**ANSWER:** Open and industry-led standards engagements allow for a wide range of industry participation while encouraging innovation and open market competition. Continued effort is needed – both at national and international levels – to identify new standards, and to harmonize, update and refine existing standards. This approach provides the greatest opportunity for all sectors to collaborate in the design, development and maintenance of industry standards to support innovation. It is critical to have the right engagement from all stakeholders, including banks, payment companies, and merchants. NIST will continue to work with these industry-led Standards Development Organizations (SDOs) where industry standards and innovative solutions for wide ranges of cybersecurity issues are addressed in an open and inclusive process. In addition, NIST will work with industry, government and academia to demonstrate cybersecurity example solutions that are based on standards and best practices.

2. On February 12<sup>th</sup>, NIST published a voluntary cybersecurity framework designed to help companies involved in critical infrastructure improve the security of their networks. It has also been reported that according to NIST, this framework isn’t a static document and that the agency has dubbed it “Version 1.0.” Please explain for us how the private sector should view this framework?

**ANSWER:** NIST believes that the private sector should view the Cybersecurity Framework as “their” Framework, as it was developed through a public-private partnership where NIST convened stakeholders. The Framework can assist in: translating cybersecurity priorities to business executives; creating and understanding cybersecurity programs; and communicating cybersecurity capabilities, needs and requirements to suppliers, partners and customers. NIST plans to continue this public-private partnership to ensure the Cybersecurity Framework remains up to date and prepares public and

private sector entities to meet the changing threat and technology environments in which the private sector operates in the future.

3. Will critical infrastructure companies use the NIST Framework?

**ANSWER:** Many critical infrastructure companies are already using the Cybersecurity Framework to implement cybersecurity programs, improve existing programs, communicate requirements and discuss cybersecurity with business executives. NIST is working alongside DHS to support further use of the Cybersecurity Framework, and to ensure that it continues to meet the objectives laid out in Executive Order 13636.

a. Could the NIST Framework be used by sectors other than critical infrastructure?

**ANSWER:** Yes, the Cybersecurity Framework can be used by a range of entities. It was designed for the urgent mission of better ensuring critical infrastructure, but it is also available to other private sector entities. The Cybersecurity Framework is designed to be flexible, risk-based and used by organizations with different business models, different technology, and different threat models. This is a critical piece given that Cybersecurity Framework needs to be both effective and consistent across the differing critical infrastructure sectors. We believe these qualities also allow the Cybersecurity Framework to be used by sectors other than critical infrastructure.

4. Solving the issue of online authentication of identity is a challenge. I understand businesses have been working for years on providing different online identity schemes to consumers, and that the Administration's National Strategy for Trusted Identities in Cyberspace (NSTIC) is also working on consensus policies, technologies and standards for online identities.

a. How can the Federal government support stronger identity management?

**ANSWER:** There are three things the Federal government can do.

First, continue to support the external-facing (i.e., non-government) aspects of NSTIC implementation – namely ongoing NSTIC pilots that are demonstrating improved online identity approaches, as well as the Identity Ecosystem Steering Group (IDESG) – a privately-led organization that is working cooperatively with the government to build a framework of standards, policies and business rules that will provide a foundation for the Identity Ecosystem.

Second, the Federal Government could accelerate efforts to embrace NSTIC at our Federal sites – leveraging approved trusted credentials to enable new types of citizen-facing online transactions in a way that improves security, privacy and convenience for citizens. NSTIC directs agencies to follow the Federal Identity Credential and Access Management (FICAM) Roadmap, crafted by the Federal Chief Information Officers Council, including making use of third party credentials issued by firms and organizations approved through the General Services Administration's FICAM Trust Framework Solutions (TFS) program. Key to accelerating these efforts is successful deployment and adoption by all agencies of the Federal Cloud Credential Exchange (FCCX). FCCX provides a shared

infrastructure that provides agencies with an “easy button” to integrate with the growing marketplace of government-approved, strong identity solutions in a way that enhances privacy and allows a citizen to use a single credential across multiple government sites.

Third, the Federal government can consider ways to address policy gaps that may serve as a disincentive for the private sector to embrace better identity solutions. Through implementing NSTIC, we have learned from many private sector stakeholders that uncertainty about issues such as liability and privacy are hindering the private sector from embracing better online identity and authentication tools. New policies in these areas may help to clarify the legal and regulatory landscape and enable widespread adoption of better identity solutions.

Together, these three Federal efforts could, within a few years, catalyze a marketplace where all of us would be able to choose from a variety of identity solutions for online login that is more secure, convenient and privacy-enhancing than the password-based systems we use today.

b. How do we ensure privacy?

ANSWER: NSTIC calls out privacy as a guiding principle, and specifically calls out the need for all identity solutions to be privacy-enhancing and voluntary. On a technical level, that requires that identity solutions adopt a “privacy by design” approach – taking the time up front to build privacy into the solution architectures. The Federal Cloud Credential Exchange (FCCX), for example, employs a “double blind” architecture which ensures that firms and organizations providing credentialing solutions have zero visibility into which agencies people are logging into; likewise, agencies cannot track what other sites people log into. This approach makes tracking technically impossible.

Beyond the technical layer, there is also a policy layer. The privately-led Identity Ecosystem Steering Group (IDESG) has a Privacy Committee that has an essential role in privacy, with participants from a number of major privacy and consumer advocacy organizations; IDESG rules require the committee to review all deliverables – and for other committees to liaise with them early on to ensure that privacy is built in to all deliverables from the start.

c. What prevents this effort from eventually resulting in regulations that inhibit innovation?

ANSWER: NSTIC is a strategy and does not call for regulation; it specifically calls for the private sector to lead its implementation – and the private sector has risen to the challenge, with active participation in the privately-led Identity Ecosystem Steering Group (IDESG) and NSTIC pilots. The Administration has not proposed any regulations around NSTIC, and none are anticipated. Of note, the IDESG itself has a policy committee of private sector members that have identified several areas where legislation or regulation could create better incentives for the private sector to improve identity management efforts, but these ideas are focused on policy concepts that would create a framework to encourage innovation.

5. What do you consider to be the greatest data security challenges today and in the future?

**ANSWER:** With new technologies that can improve our quality of life come associated risks. For the future, we are performing research and development to understand the associated risks of future technologies so that effective, safe and appropriate use can emerge along with those innovations. We will continue to work with industry, academia, and internationally to support the development of products where cybersecurity is a default setting, is easy to use and understand, and supports the purposes of the technology. Waiting to address cybersecurity after technology deployment should no longer be considered acceptable.

6. What is the fastest and best way to get new innovations deployed to protect the safety, privacy, and security of consumers' financial data: government mandates that would pick technology winners and losers, or, allowing maximum competition for customers in the market by companies offering innovative security solutions and consumer protections against new, evolving, and changing threats that go beyond the requirements of a static law?

**ANSWER:** Industry-led and government participating standards development in accredited Standards Development Organizations gives maximum competition for customers through interoperable standards for multiple product participation. This fosters innovation with open and competitive markets leveraging common standards as a base for new products to integrate into existing environments. It allows for new products that can deliver needed security, privacy controls, and product safety in times of evolving threats, business needs and risks.

**Questions submitted by Rep. David Schweikert**

1. Given that the NIST framework is wholly voluntary, and the framework itself contains no direct means by which to enforce compliance, what measures can Congress use to best ensure institutions are meeting the cyber security needs to best protect Americans, be they tax incentives, preference in government contracting, or something else?

**ANSWER:** The Cybersecurity Framework was the result of a strong public-private partnership. This established an open and honest dialog on challenges and capabilities in a non-regulatory atmosphere. Many critical infrastructure companies are already using the Cybersecurity Framework to create cybersecurity programs, improve existing programs, communicate requirements and discuss cybersecurity with business executives. Encouragement of public-private partnerships where the best of government, industry, academia and international stakeholders come together to address this national need and allowing for markets to emerge and support its use is how we have seen success in this work.

2. One of the concepts floated has been to amend the SAFETY Act of 2002, by adding a cyber-technology application and providing liability protection to companies using certified cyber-technology or systems. Would this lead to faster adoption of cyber security principles?

**ANSWER:** When discussing changes to the SAFETY Act of 2002, the impacts to policy, implementation, and resources must be carefully considered to ensure that the effective functioning of the SAFETY Act program can be maintained. Specifically, any lowering of the threshold for liability protection for cyber technologies may result in the bar being raised for providing eligibility for the related protections. For these reasons, language related to determining when a qualifying cyber incident has occurred must also be carefully considered.

In August of last year, NIST contributed to a Department of Commerce Internet Policy Task Force (IPTF) paper on incentives that affect cybersecurity practices. This report began with a Notice of Inquiry asking stakeholders for input on a broad array of questions. Based on responses to this NOI, previous input to the Commerce IPTF, consultations with other federal departments and agencies, and related analysis, the IPTF made preliminary recommendations to the President on potential actions that the U.S. Government can take to build a successful incentives structure for the Program, including further analysis of the "legal and financial risks that critical infrastructure owners and operators face from tort liabilities arising out of cyber-attacks." That report is available online ([http://www.ntia.doc.gov/files/ntia/Commerce\\_Incentives\\_Discussion\\_Final.pdf](http://www.ntia.doc.gov/files/ntia/Commerce_Incentives_Discussion_Final.pdf)).

<sup>(3)</sup> In conjunction with the Department of Homeland Security's Critical Infrastructure Cyber Community (C<sup>3</sup>) Voluntary Program and its encouragement of the Cybersecurity Framework, eight incentives are being discussed among Federal agencies as well as industry stakeholders. Some of the recommended incentives can be implemented within current authorities as part of the C<sup>3</sup> Voluntary Program, while others may require legislative action. As of today these policy levers are still under advisement.

*Responses by Mr. Bob Russo*

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY  
SUBCOMMITTEE ON OVERSIGHT  
AND  
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

**“Can Technology Protect Americans from International Cybercriminals?”**

**March 6, 2014**

**QUESTIONS FOR THE RECORD**

**Mr. Bob Russo**

**General Manager, Payment Card Industry Security Standards Council, LLC**

**Questions submitted by Chairman Broun and Chairman Bueshon**

- 1. What can we do to protect patient privacy and ensure that there is sufficient security to protect patient records in the healthcare and insurance industries?**

The PCI Security Standards Council (“the Council”) developed the PCI Security Standards to specifically protect consumers’ payment card data, not patient healthcare or insurance information. The PCI Data Security Standard (“PCI DSS”) applies to any entity that stores, transmits, or processes payment card data. The Council’s mission is not focused on security of other types of data. However we believe our security standards are a strong baseline that may be adapted by other industries for use in protecting other types of sensitive data. Security principles and methods included in the PCI Data Security Standard (PCI DSS) for example, include widely acknowledged security measures such as changing default passwords and educating staff on how to protect sensitive information.

- 2. What can PCI or other cyber-engaged entities do to help banks, payment companies and merchants better collaborate on industry standards and innovative solutions to data breaches and cybercrime for electronic financial transactions?**

The Council is a good example of the type of organization that enables multiple stakeholders to collaborate on innovative solutions for data breaches and cybercrime. With membership of over 1,000 participating companies worldwide, we are the premier open global forum for the protection of payment card data. We encourage all entities that store, process or transmit payment card data to join us in our work to improve the security of this information. In addition to our collaborative development process for enhancing security standards, other initiatives led by the PCI Council that foster information sharing and collaboration include number of special interest groups and task forces that solicit industry expertise for tackling specific challenges in payment security; training sessions that bring together industry participants, an outreach effort that develops and promotes payment security focused content. In addition the Council provides the opportunity for payment applications, PIN transaction security devices and point to point encryption solutions space to be validated by Council approved laboratories and listed on our

public website. Other information sharing vehicles exist in the form of the FS-ISAC. The Council commends and encourages the continuation of this work.

**3. What steps can be taken to fix the cybersecurity crisis in the healthcare and insurance industry?**

The PCI Security Standards Council is specifically focused on securing payment card data wherever it is stored, processed or transmitted. Our remit does not cover patient data, healthcare or insurance information. As noted, we believe our security standards are a strong baseline for protecting payment card data. Other industries may also adapt and benefit from the security measures and practices recommended in PCI Standards.

**4. When a vendor falls victim to a cyber-security breach, in how many cases have you identified the cause to be a failure in PCI compliance?**

**a. How can there be a failure when they are considered to be PCI-certified to begin with?**

There are many reasons that an organization may experience a breach ranging from being a victim of a new inventive exploit, to failing to implement adequate security protocols or act on alerts in their PCI program.

As a technical standards body, the Council is not involved in enforcement and therefore does not directly track, participate in, or monitor breach investigations. However, most public information on breaches shared in industry reports from companies such as Verizon or Trustwave, indicate failures in basic security protocols that are emphasized in PCI Standards.

Security is a dynamic business, not a static state. Companies should expend their energy, resource and budget on creating and maintaining a robust security program that protects payment card data around the clock, not just at an assessment which is one point in time. Just as a company could be certified as being protected against a fire because they have smoke detectors, they could find themselves vulnerable at a later time if they do not change the batteries. Security requires round the clock effort, it does not end on the day a positive mark is received on a certification audit.

Organizations that protect payment card data through a strong security program based on PCI Standards improve their chances both of avoiding a breach in the first place, and of minimizing the resulting damage if they are breached. No one standard, mandate or technology is a silver bullet for payment data security. PCI standards are one part of multi-layered security program that should combine people, process and technology.

**5. Is it easier for international cybercriminals to perform a targeted attack on a Fortune 100 company or on small and medium enterprises?**

- a. Are all vendors required to follow the same standards, or are there differences between larger businesses versus smaller ones, which may not have as much available funding for the latest technology?**

Since each individual organization – regardless of size- has a different IT and payment processing environment it is difficult to generalize. It's true that larger companies may have more resources to expend on payment security, but they also may have more complex environments. Smaller enterprises may have fewer resources or limited expertise in this area, but they may also completely outsource payment processing to a third party provider. Although it is difficult to generalize, it can be expected that criminals are going to go where they can get the biggest reward for their efforts – the most data. For this reason large merchants and service providers are a target.

All organizations that store, process or transmit payment card data are subject to the same PCI Data Security Standard. The difference lies in how an organization reports its compliance with the standard to its acquirer and/or payment brand since the role of the Council does not include compliance validation, reporting or tracking. An organization that accepts a large number of payment card transactions may be subject to an annual assessment of its systems. A smaller company may be required to complete a self-assessment questionnaire to understand and communicate its security posture with any business partners.

**6. What do you consider to be the greatest data security challenges today and in the future?**

With regard to payment card data security, the Council considers the increasing sophistication of global cybercrime to be the greatest threat today. We have every reason to believe that the criminal elements that focus on attacking systems to access payment card data will continue to organize and innovate in the future. Strong law enforcement and industry- led initiatives to raise awareness will remain critical in protecting consumers' confidential payment information.

- 7. When a merchant or vendor experiences a cyber-attack, to what extent, if any, do they share the lessons learned from this experience with other businesses?**
- a. What are some of the obstacles to such sharing of information and can they be overcome?**

Information sharing is a critical part of security, and the Council supports responsible efforts to enhance the sharing of information among stakeholders in the payment chain.

One consideration is that organizations that experience data compromise are often constrained in sharing information publicly during pending law enforcement and forensics investigations. This

is often due to the desire to avoid sharing incomplete or inaccurate information before a comprehensive investigation is complete, to avoid complications regarding potential litigation, or to avoid impeding an ongoing investigation.

The Council regularly looks to share information and lessons from the threats merchants and financial intuitions are facing in our community. Our Board of Advisors is comprised of many retailers, financial institutions and processors and will regularly discuss emerging threats. Our PCI Forensic Investigator (PFI) program, in which forensics investigators share anonymous compromise trend information on a quarterly basis in a series of face to face meetings with the Council, has also been useful in this regard.

We utilize this shared information to refine the standard and adapt our training, as well as to issue periodic information supplements when we feel that we can be useful in helping the marketplace understand the nature of emerging threats

8. **What is the fastest and best way to get new innovations deployed to protect the safety, privacy, and security of consumers' financial data: government mandates that would pick technology winners and losers, or, allowing maximum competition for customers in the market by companies offering innovative security solutions and consumer protections against new, evolving, and changing threats that go beyond the requirements of a static law?**

With regard to payment card data, the government can play a role through awareness raising, streamlining data breach notification laws, improving public-private collaboration, and encouraging information sharing and through supporting strong law enforcement.

The Council strongly believes in the dynamism of the marketplace to continue to innovate in payment and security technologies and processes. We believe market driven standards, developed and continually enhanced by industry experts, practitioners and leading innovators, are the best approach to encouraging a multi-layered approach to security that provides a strong foundation for adoption of new technologies.

**Questions submitted by Ranking Member Maffei**

- 1. In 2013 around 11-percent of companies in the Payment Card Industry were “fully compliant” with your organizations “Data Security Standard,” but back in 2010, 22-percent of companies surveyed were “fully compliant.” Can you offer any insight into why that is? Why do you believe there are so few companies that are fully compliant with this security standard, why has the rate of compliance dropped in recent years and what do you think can be done to help persuade companies to be more diligent about applying proven security standards to their networks?**

*Note for the record: Data in the above question is drawn from the 2011 and 2014 Verizon PCI Reports.*

These statistics refer to a baseline assessment of an organization’s PCI Data Security Standard compliance status at the time a Verizon assessor first looks at an organization’s systems. From this point on, organizations work with their security providers to achieve full compliance. This year’s Verizon PCI Compliance Report cites the following:

- Baseline or “first look” assessment of compliance increased from 7.5% in 2012 to 11% in 2013

The percentage of organizations that were “nearly there” or close to achieving full compliance in this initial “first look” at their systems dramatically increased:

- “Just over 70% of organizations that we assessed in 2013 were “nearly there” — complying with 81-99% of controls — up from 25% in 2012. This represents significant progress in the number of companies that are implementing PCI Security as business as usual.”

The report additionally states that they “continue to see many organizations viewing PCI compliance as a single annual event, unaware that compliance needs to have a 365 day-a-year focus.” The Council continues to remind organizations that proper implementation and ongoing maintenance are critical to protecting card data, and the most recent release of the PCI DSS includes an increased focus on helping organizations prioritize a business-as-usual approach to payment card security. To this end the Council, through feedback from the community has worked to improve the usability of the latest version of the PCI DSS to ensure it is followed year round. For example we introduced a new section into PCI DSS 3.0 entitled “Best practices for implementing security into business-as-usual to maintain ongoing PCI DSS compliance”. The Council also incorporated security policies and operational procedures from requirement 12 throughout the entire PCI DSS 3.0.

As a clarification for the record, the Council is responsible for technical standards development, not for enforcing or monitoring compliance. This responsibility is owned by acquiring banks and

card brands. Publicly available statistics about some of the largest merchants and service providers in the USA paints a different picture. Other public sources of PCI DSS compliance, such as this one from Visa show that 97% of large merchants reported PCI compliance to Visa in 2013.

It should also be noted that Verizon is just one assessment and forensics company. While it's report is important, the data included within does not represent the entire merchant or service provider population of the United States.

- 2. In your testimony you said that data security standards were the “best line of defense against criminals seeking to steal payment card data.” But these are all voluntary standards. If only 10 or even 20-percent of industry is “fully compliant” do you believe that the federal government should either mandate or help incentivize compliance with security standards?**

The Council supports the federal government's work to raise awareness of the importance of strong payment card data security. Since adopting PCI Standards is typically included in a business contract between merchant, service provider and their bank, compliance is not voluntary. For reasons noted in this response the Council believes incentives from the federal government, rather than mandates would be more appropriate.

*Responses by Mr. Randy Vanderhoof*

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY  
SUBCOMMITTEE ON OVERSIGHT  
AND  
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

**“Can Technology Protect Americans from International Cybercriminals?”**

**QUESTIONS FOR THE RECORD**

**Mr. Randy Vanderhoof, Executive Director, Smart Card Alliance**

**Questions submitted by Chairman Broun and Chairman Bucshon**

- 1. What can we do to protect patient privacy and ensure that there is sufficient security to protect patient records in the healthcare and insurance industries?**
- 4. What steps can be taken to fix the cybersecurity crisis in the healthcare and insurance industry?**

In healthcare and insurance, protecting patient privacy and patient data is critical. Healthcare organizations are increasingly under attack by cybercriminals seeking to gain access to patient data and to Internet-connected medical devices. Sometimes, seemingly small events, like the loss of a laptop or a USB device, can lead to thousands or even millions of compromised patient records.

A single compromised medical record sells for \$50 and can be used to commit medical identity theft. The average cost to resolve a single case is \$20,663. A recent study estimates that nearly 1.5 million Americans are victims of medical identity theft. In 63 percent of the cases, the victim's name was used to obtain medical treatment or service, and in 43 percent, the victim's name was used to obtain government benefits such as Medicare and Medicaid.

The way to improve the security of healthcare patients and data is to strengthen our identity management processes. Identity management is a crucial foundation for healthcare, and solutions that incorporate smart card technology can address the security and privacy challenges facing the industry. This foundation can be put in place without reinventing the wheel. The federal government has already established a set of best practices, standards and technology solutions for smart card-based identity management and authentication that can be adapted to and leveraged by the healthcare industry.

All personal health record (PHR) providers, health record banks, health insurance and hospital Web portals should provide two-factor authentication mechanisms to their end users to help secure access to personal health information. In two-factor authentication schemes, individuals typically use a card, token or mobile device to access their health information or prove identity when obtaining healthcare services. The safest and most secure two-factor methods are based on smart card technology, where a tamper-resistant chip with security software is embedded into the card, token or mobile device (like a mobile phone). This is the same technology that is used in U.S. electronic passports and in the U.S. federal government's employee ID cards that are used to access the nation's most secure computer networks and facilities. A smart card allows patients to unambiguously identify themselves to their healthcare provider when accessing patient records or requesting healthcare services.

Data encryption also plays an important role in the protection of personal health information (PHI) and is now mandated as part of the breach notification laws. Encrypting PHI protects against access by

intruders; smart cards provide a robust set of encryption-enabling capabilities including key generation, secure key storage, hashing and digital signing. Smart cards also add strong authentication capabilities that ensure only authorized users are able to access PHI.

These capabilities can be used by a healthcare system to protect privacy in a number of ways. A doctor can use a smart card to digitally sign orders or prescriptions, protecting the information from subsequently being tampered with and providing assurance that the doctor was the originator of the information. The fact that the signing key originated from a smart card adds credibility and a greater legal stature to the record. The smart card provides two major benefits: it securely holds and protects the keys, and it is portable, so it stays with the doctor and not in the computer where someone else might be able to fraudulently use it. Smart cards can also put patients in control of their private information. Patients can use their smart card to securely store personal health information, authorize provider access to that information and secure transmission of data to healthcare systems.

2. **If a hack similar to Target occurs at a retailer where new chip cards are used, what kind of information would cybercriminals be able to obtain and how profitable or devalued would such information be for these criminals?**

If a hack, similar to those at Target, Neiman Marcus and other retailers, were to occur in a retail environment with chip card data, the information obtained would be different and less useful for counterfeiting than the information obtained from magnetic stripe cards.

The information obtained from magnetic stripe payment data can include the primary account number (PAN), card expiration date and a card verification value (CVV). The CVV used for a magnetic stripe transaction is static, meaning it never changes. This is why it is easy for fraudsters to take this information and create useable counterfeit magnetic stripe cards.

Chip card data has a very important distinction: it does not use static CVVs like magnetic stripe cards. Instead, it uses a dynamic, one-time use security code known as the iCVV. This means that if a criminal were to obtain chip card data and clone it onto a counterfeit card, any transactions attempted with that card would be declined. For this reason, chip cards greatly devalue the transaction data passed to merchants in the eyes of criminals, giving them little incentive to go after it for counterfeit card fraud purposes.

It is also worth noting that chip cards have other features that protect against counterfeit card fraud. The chip itself is a powerful microcomputer with active defenses that prevent tampering with the application and the information it stores inside its memory. Even if chip data were to be copied, it could not be used to create a usable copy onto another chip card because each chip is programmed with a secret key known only to the issuer. The less secure magnetic stripe has no defenses to prevent a criminal from reading the stripe and reprogramming that same card data onto another magnetic stripe, creating an undetectable copy of the original card.

3. **What can Smart Card Alliance or other cyber-engaged entities do to help banks, payment companies and merchants better collaborate on industry standards and innovative solutions to data breaches and cybercrime for electronic financial transactions?**

Industry groups, such as the Smart Card Alliance, are able to convene subject matter experts with a deep understanding of the technical challenges and business issues related to addressing the challenges of data breaches and financial security. As an example, the Smart Card Alliance started looking into the EMV chip card standards to replace magnetic stripe cards nearly two years before the global payments brands announced their plans to migrate the U.S. market to chip cards. To help facilitate a successful migration, the Alliance created a dedicated group, the EMV Migration Forum, to address topics that require some level of industry cooperation and/or coordination. Through industry-led, collaborative working committees under the guidance of experienced senior people in the financial industry, both groups have published and distributed educational white papers that examine the payments security challenges from a technical and business perspective and have proposed multiple approaches to address security problems.

The Smart Card Alliance's EMV Roadmap white paper, "[Card Payments Roadmap in the U.S.: How Will EMV Impact the Future Payments Infrastructure?](#)" and subsequent webinars and payments conference events helped explain how chip technology made payments more secure. The Alliance also explained how the changes would impact all payments stakeholders. These resources have helped shape the business and technical decisions that are happening now that will remove magnetic stripe data from the market over time, reduce the likelihood of future data breaches and accelerate the changes to the payments acceptance and processing networks. These changes resulting from the migration to chip technology will enable the advancement of the next generation of layered security innovations such as tokenization, encryption and mobile transactions to be introduced in the near future.

Currently, there is no single approach to securing the payments market that would meet every need and also be economically viable. Instead, a layered approach to security is often the best approach. Industry groups can draw on experiences from other stakeholder groups and from other countries, to make informed judgments on how their solutions and approaches might fit with the unique market dynamics that exists in the U.S.

**4. What do you consider to be the greatest data security challenges today and in the future? Mike Smith**

Identity in all its forms is, and will continue to be, the greatest data security challenge for people and businesses. For the 14<sup>th</sup> year, identity theft continues to top the Federal Trade Commission's national ranking of consumer complaints. The EMV chip card initiative will help. In the latest data available from the Bureau of Justice Statistics, seven percent (8.6 million) of U.S. households experienced identity theft victimization and of those, 64 percent involved credit card accounts. But with the growth of Internet and mobile commerce, digital identity has also become a challenge. Passwords and shared secrets are too easily compromised. Smart cards can be used to create a vetted digital identity to strongly authenticate across multiple domains, not only in payments, but also in mobile phones, drivers' licenses or federal ID cards for Social Security or Medicare. Determining appropriate security and risk liability tradeoffs for identity providers to help such ecosystems flourish is a fundamental issue.

**5. Do you believe that cybercriminals will increasingly take advantage of the less secure magnetic stripe card technology to electronically steal payment data from U.S. industries before the October 2015 transition to chip cards and readers? In other words, is the window of opportunity on magnetic stripe cards closing on cybercriminals?**

It is unclear whether retailer breaches will increase, but it is important to move to chip technology to reduce the possibility. For some time now, the U.S. payments industry has been operating under an elevated threat level, with the understanding that magnetic stripe payment data makes the U.S. a target for counterfeit card fraudsters. The recent breaches at Target, Neiman Marcus and other retailers heightened awareness of the threat and strengthened the resolve of the payments industry to close this “window of opportunity” and introduce EMV chip payments as quickly as possible.

The migration to chip payments in the U.S., which is the largest market to ever migrate to EMV chip payments, is a significant and complex undertaking. Because of this, the October 2015 target date presents a reasonable but aggressive timeline for a market this size. Today, approximately two years into the migration, substantial progress has been made. With issuers, acquirers and merchants committed to the technology and readying their organizations, this progress will continue to accelerate. To date, we have approximately 17 to 20 million EMV chip cards in the field, and millions of in-store POS terminals and ATMs ready to accept chip payments. These numbers are likely to increase by one hundred million cards or more in the next year, while the number of chip-capable POS terminals and ATMs could double or even triple. What the industry is striving for in the coming years, and what will close the counterfeit fraud opportunity, is for the majority of our transactions to be made with chip cards on chip-enabled terminals.

**6. Once chip cards are implemented in the U.S., do you believe there will be an increase in online breaches? Are retailers preparing for such a possibility?**

We don’t know of evidence from other countries that have migrated to EMV chip cards that shows that data breaches at online e-commerce merchants increase as a result of implementing chip cards to address card-present counterfeit card fraud.

The dynamic data generated by EMV chip cards and the omission of data used in magnetic stripe transactions greatly devalue any payment data that is present in the retailer’s or third party processor systems since the chip data cannot be made into counterfeit cards to commit fraud. It is also important to note that EMV transaction data does not include the card security code that is printed on the card and that is used in an online e-commerce transaction. Once the country has migrated to EMV, it is conceivable that physical merchant data breaches will decline since any data stolen won’t be useful to create counterfeit cards.

Online e-commerce transactions do not use EMV chip cards; consumers simply enter their payment card account information. Like physical merchants, online e-commerce merchants must comply with the Payment Card Industry Data Security Standard (PCI DSS) to protect cardholder information. Once the country has migrated to EMV, any data stolen from an online merchant would not be usable to create counterfeit chip cards, reducing the value of breaches for fraudsters.

The industry understands the risk of online e-commerce transactions and the need for securing cardholder information. One important approach that helps to address both data breaches and online e-commerce fraud is “tokenization” where cardholder information is replaced with a “token” that is then used for transactions at a specific merchant. Tokenization eliminates sensitive cardholder information from the merchant’s environment and tokens are not usable by fraudsters since they can’t be used anywhere except at the merchant which originated the token. Commercial tokenization solutions are now being used by the payments industry, and EMVCo has launched an accelerated effort to develop a tokenization standard.

I would note that experience in other countries has found that as counterfeit card fraud declines, fraud in other channels such as online e-commerce or telephone/mail order channels, and card-not-present (CNP) fraud (i.e., the unauthorized use of a credit or debit card number to purchase products or services in a setting where the customer and merchant are not interacting face-to-face) increases as a proportion of total fraud. Other methods are being used to address CNP fraud; these are summarized in question #11 below.

**7. What is the value - financial and personal - of stealing magnetic strip card data versus chip and PIN card data?**

The financial value of magnetic stripe data is higher than that of chip card data for criminal activity because it can be used to create and successfully use counterfeit payments cards. For example the several million card accounts stolen during the Target breach sold on the black market for between \$26.60 and \$44.80 each prior to Dec. 19, 2013. Because chip card data cannot be used to create usable counterfeit cards, its value is less. There have been documented instances of criminals bypassing or throwing out chip card data in favor of magnetic stripe data.

The personal data value of stolen magnetic stripe card data and chip card data is minimal, as the data does not include the cardholder's personal details.

**a. Does a hacker get more information from a magnetic strip card than a chip card?**

Hackers get more usable information for criminal counterfeiting activity from magnetic stripe cards than chip cards. The transaction data from a magnetic stripe transactions can include some or all of the following: the primary account number (PAN), card expiration date and a card verification value (CVV). Armed with this information, criminals can create and successfully use counterfeit magnetic stripe cards.

Chip card transaction data is much less valuable to criminals for counterfeiting because it contains a dynamic, one-time use security code and it does not include the magnetic stripe version of the CVV. This means that even if criminals are somehow able to obtain this information, they cannot use it to create a usable counterfeit chip card.

**b. If someone tried to duplicate information from a chip card that had a magnetic stripe on it to make a duplicate magnetic stripe card, would that duplicate card work at retailers?**

No, that transaction would not be successful at a retailer that accepts chip payments. When issued on a chip card, a magnetic stripe has different information stored on it than a traditional magnetic stripe-only card. In this scenario, a chip card's magnetic stripe is copied and a card is created with that card's data written to another magnetic stripe on an unauthorized second card. When that counterfeit card is swiped at a merchant terminal that can process a chip transaction, the terminal would direct the customer to use the chip. Because the chip doesn't exist on this counterfeit card, the transaction will be declined by the issuer. If the counterfeit card is used at a terminal that does not support a chip, the card would be accepted unless the issuer flags the transaction based on certain usage analytics or if the cardholder reported the card lost or stolen.

**8. You mention in your testimony that, "the issuance of chip cards in the U.S. does not mean the elimination of the magnetic stripe altogether." Randy Vanderhoof**

**a. How long do you think it will take for the United States to fully implement chip cards and be completely rid of any magnetic stripes on cards?**

Industry leaders are firmly behind the efforts to make payments more secure, reduce the likelihood of more data breaches and lessen the damage caused for issuers, merchants and consumers when crimes against payment products occur. However, it is also important to implement these security improvements without significantly inconveniencing consumers and retailers and adding friction to consumer spending. Magnetic stripes are still the lowest common denominator for card payments globally. Eliminating all magnetic stripes from cards will take years, if ever, to achieve. Even though Europe is ten years ahead of the U.S. in chip cards, 20 percent of their cards still use magnetic stripes.

The issuers of payments cards and the merchants who accept those cards are not mandated to adopt the EMV chip standard. The global brands who determine rules for fraud risk can adjust those rules to protect the more secure party (either the issuer or the merchant, since the consumer is protected either way) involved in the transaction when fraud occurs, but cannot mandate that the chip be present and accepted for every transaction. It is expected that magnetic stripe-only cards and magnetic stripe-only accepting terminals will be around for many years, but in increasingly smaller numbers. The more important metric, and what the U.S. industry is striving for, is to increase the percentage of "chip on chip" transactions (a chip card payment accepted by a chip-enabled terminal) over time until they make up the majority of our transactions.

**b. Do these magnetic stripes on a chip and PIN card pose a similar fraud concern as our current magnetic-stripe-only credit and debit cards do?**

The magnetic stripes that will remain on the backs of bank-issued EMV chip cards do not pose a fraud threat to card issuers or consumers once chip-enabled merchant terminals programmed for EMV chip card acceptance are widely deployed. When issued on a chip card, a magnetic stripe has different information encoded on that stripe than do magnetic-stripe-only cards. When an EMV chip-issued card is swiped at an EMV chip-accepting terminal, it signals to the terminal that the card was issued with a chip. The terminal will then force the card to be used as a more secure chip card rather than as a less secure magnetic stripe card at that device.

In one scenario, a chip card's magnetic stripe is copied and a card is created with that card's data written to another magnetic stripe on an unauthorized second card. When that counterfeit card is swiped at a merchant terminal that can process a chip transaction, the terminal would direct the customer to use the chip. Because the chip doesn't exist on this counterfeit card, the transaction will be declined by the issuer. In a second scenario where the counterfeit card is used at a terminal that does not support a chip, the card would be accepted unless the issuer flags the transaction based on certain usage analytics or if the cardholder reported the card lost or stolen.

**9. If chip cards are a first step to decreasing fraud in the United States, what is the next vulnerability that might need to be confronted by industry?**

Experience in other countries has found that as counterfeit card fraud declines, fraudsters move to other channels. Outside of the U.S., this has included fraud in card-not-present transactions, ATM fraud (when ATM migration has lagged POS terminal migration) and cross-border counterfeit card fraud (where stolen payment credentials are used in countries that have not migrated to chip cards and chip-enabled POS terminals). It is important to look at the overall payments ecosystem when considering

next vulnerabilities. As technologies improve security for card payments, it is conceivable that fraudsters may move to other payment types – for example, ACH channels – as another avenue for cybercrime.

**10. While chip cards provide fraud protection from counterfeit cards used in physical retail stores, what technologies or solutions are being considered to fight ‘card not present’ fraud in the online retail channels? *Cathy Medich***

Online e-commerce merchants and the payments industry currently take a variety of approaches to authenticate consumers during card-not-present (CNP) transactions to help mitigate against CNP fraud. Some general classes of approaches include static or random passwords, dynamic information such as one-time passwords generated in software or using a smart card or mobile phone, knowledge-based approaches (such as asking secret questions) and device fingerprinting, where some information is used to identify the device by which the user is accessing an e-commerce site.

The payments industry has implemented a number of standard approaches for CNP authentication. Asking for the cardholder’s zip code for address verification and entering the “card security code” printed on the card are common methods used by many, but not all, merchants. Card issuers validate that this information is correct during the transaction authorization. The payments networks have also defined other standard CNP authentication protocols that are in use internationally. MasterCard and Visa both have programs outside of the U.S. that use EMV payment cards and cardholder readers to generate one-time passwords for online access. The 3D Secure software protocol is also in use by merchants and issuers to validate cardholder identity during an e-commerce transaction. Looking at Europe’s experience, the UK Cards Association reported a one-third drop in CNP fraud since 2007 due to increasing use of fraud screening tools and 3D Secure.

Online e-commerce merchants typically implement multiple solutions to mitigate CNP fraud or use a commercial service to mitigate transaction risk. Since merchants today assume the costs of CNP fraud as well as typically pay higher fees for e-commerce transactions, merchants also may have their own internal fraud departments and often use tools to score the risk of online shopping behavior to determine which online purchases to accept, reject or send for review.

It is important to note that merchants are very sensitive to any security that is going to make check-out more difficult for shoppers. Some very secure methods proposed to merchants have not been adopted because they cost them business. They are afraid of higher shopping cart abandonment rates when they ask additional security questions or require extra steps of customers to authenticate themselves. They don’t want to lose a sale because they made it too hard for customers to complete the checkout process. Ultimately, online e-commerce retailers have to balance the risk of losses due to fraud with making the purchase process more difficult for the consumer. So each e-commerce merchant will take different approaches based on its transaction volume and potential for fraud.

The payments industry understands that CNP fraud is a significant issue. The effort to standardize the approach for tokenization (see question 7) is one initiative that is expected to help address CNP fraud. To educate stakeholders on CNP fraud, the Smart Card Alliance Payments Council published a white paper, [“Card-Not-Present Fraud: A Primer on Trends and Authentication Processes,”](#) in February 2014. In addition, the EMV Migration Forum’s Card-Not-Present Fraud Working Committee has been engaging merchants, issuers, payment brands and technology suppliers in discussion to identify and agree on best practices for mitigating against CNP fraud. Their goal is to publish a white paper later this year and start

to educate the market on best practices for authenticating the cardholder for online e-commerce transactions.

**11. When a merchant or vendor experiences a cyber-attack, to what extent, if any, do they share the lessons learned from this experience with other businesses?**

Generally speaking, when a merchant or payments industry vendor becomes aware of a data breach or malware attack, the first step is to bring in forensic data security experts to determine the cause of the breach and fix the problem. The next step is to inform law enforcement about the breach so that they can try to identify who was behind the attack. The steps after that vary depending on the size of the breach and the extent of the damage that may have resulted from the data being stolen. This could lead to notifications of their payments processor and other third party vendors involved in the compromised system. Rarely does it involve public sharing of information with other organizations, but more organizations are seeing the value in this and joining information-sharing groups to share experiences and lessons learned.

Payment industry organizations today are increasingly interested in information sharing after data breaches. After its breach, Target joined the Financial Services Information Sharing & Analysis Center (FS-ISAC), a non-profit private sector initiative developed by the financial services industry to help facilitate the detection, prevention and response to cyberattacks and fraud activity. Heartland Payments System, another organization that suffered a major breach, is also a member and helped form the Payments Processing Information Sharing Council (PPISC). According to the National Retail Federation (NRF), the retail industry is considering many different proposals and options aimed at identifying, preventing and combating coordinated cyberattacks, including the establishment of a retail industry Information Sharing and Analysis Center, or ISAC.

**a. What are some of the obstacles to such sharing of information and can they be overcome?**

Some of the obstacles for sharing information include:

- Legal concerns over liability
- Damage to company reputation and loss of consumer confidence
- The time it takes to understand the nature of the attack and any unique factors that may have contributed, like insider activity, faulty hardware or software, or a combination of internal factors

Because of these obstacles, other industry parties who might be equally vulnerable may never hear about what happened and how it occurred. Groups that are organized and led by the industry, like the FS-ISAC or the proposed ISAC for the retail industry, present important opportunities for organizations to share information in order to prevent cyberattacks.

**12. What is the fastest and best way to get new innovations deployed to protect the safety, privacy, and security of consumers' financial data: government mandates that would pick technology winners and losers, or, allowing maximum competition for customers in the market by companies offering innovative security solutions and consumer protections against new, evolving, and changing threats that go beyond the requirements of a static law?**

The market should be allowed to figure out what works best for the industry to protect the security of financial data while being in compliance with regulations. Regulators who have the responsibility of

protecting consumers and ensuring that industry is acting in good faith and not engaging in illegal or anti-competitive behavior should step in only if the market fails to respond in a timely and efficient way.

Today, all evidence illustrates that the U.S. payments industry is acting in good faith and is taking consumers' financial security and privacy needs seriously. The U.S. payments market is very large and complex, and the transition to a more secure ecosystem will be expensive and take considerable time to complete. The four payments brands independently set policies to encourage changes for issuers and merchants to encourage the entire market to implement EMV chip cards in a timely and coordinated fashion. It is not within the payment brands' business parameters to impose mandates or enforce compliance. Therefore, all parties involved in the activity of payments transactions need to make the necessary investments in EMV-compliant chip technology and processing in a coordinated time frame. Unless the industry moves together, the individual parties making the investments in chip technology will not see the expected return on those investments because fraudsters will continue to exploit the weakest points in the system. In my view, the industry understands this and is committed to moving forward together.

We encourage restraint in any government actions to adding additional conditions or compliance rules unless there is a major slowdown or disruption in the EMV migration process.

**Question submitted by Rep. David Schweikert**

1. **One of the reasons cited for EMV cards not being adopted sooner in America is the conversion cost, with some claiming it to be in excess of \$10 billion. The National Retail Federation claims that it could reach \$30 billion for the retail industry. How does this conversion cost compare to the cost to retailers, banks, and other financial institutions accrued from cyber-attacks and cybercrime? Randy Vanderhoof**

The NRF has not put forth any data to substantiate such a high cost that the retail industry will incur upgrading their payments acceptance hardware and software to support EMV. It can be safely assumed that the largest (Tier 1) retailers operate the most complex payments acceptance systems, therefore the costs to upgrade those systems will be significant. However, these same retailers are often the biggest targets for data breaches and counterfeit card fraud, making them major players in the highest percentage of fraud losses. The amount spent on repairing the damage due to breached systems, lost profits and fraud can ultimately be higher than the cost to upgrade to EMV chip technology.

Another important point is that retailers generally upgrade and replace their terminals and software every three to seven years as a regular business practice, so the upgrade of these systems to EMV is something they should have planned for over many years.

Issuers of payments cards also have a natural expiration and refresh cycle on these cards. The change to EMV should be measured by the extra cost of the chip cards they will be replacing when the older magnetic stripe cards expire, plus other costs associated with the new security systems in place to issue these cards and authorize them when consumers use them. As the volume of chip cards (estimated to be nearly one billion) increases, the cost per card and cost of these security services will continue to decrease.

Card-present fraud rates in the U.S. are estimated to be around \$5.6 billion per year and increasing by 10-17 percent each year, and data breaches are adding significant cost to retailers. The one-time investments for retailers and incremental investments in cards for issuers will be returned with the expected significant reduction in fraud and the risk of retail data breaches may lessen since EMV transaction data is less useful for fraudsters to steal.

*Responses by Mr. Justin Brookman*

House Committee on Science, Space, and Technology  
Subcommittee on Oversight and Subcommittee on Research and Technology

“Can Technology Protect Americans From International Cybercriminals?”

Questions for the Record to

Mr. Justin Brookman, Director, Consumer Privacy, Center for Democracy & Technology

Questions submitted by Chairman Broun and Chairman Bucshon

1. What can we do to protect patient privacy and ensure that there is sufficient security to protect patient records in the healthcare and insurance industries?

Existing state data breach notification law and the FTC’s interpretation of the FTC Act to require reasonable security have seemingly failed to provide sufficient incentives to companies to meaningfully safeguard consumer data. Congress should enact comprehensive privacy and data security legislation — with robust enforcement and penalty provisions — to provide stronger incentives to companies to safeguard consumer data, and to provide information and control to individuals to let them make informed decisions about with which entities they will share their personal information.

2. What can be done to help banks, payment companies, and merchants better collaborate on industry standards and innovative solutions to data breaches and cybercrime for electronic financial transactions?

While we believe that the incentives to safeguard personal information should be strengthened, it seems that the existing significant risks faced by companies from data breach are already not being consistently internalized across industry. Several proposed data security bills have included provisions requiring companies to enact a comprehensive data security program, to assess data security risks, and to assess the practices of third parties with whom personal information is shared. We believe that requiring companies to systematically assess and consider data security risks would encourage companies to adopt better practices, including cross-industry collaborative approaches.

3. What steps can be taken to fix the cybersecurity crisis in the healthcare and insurance industry?

We believe that data privacy and security law should be updated to require companies to adhere to the Fair Information Practice Principles: transparency, purpose specification, use limitation, data minimization, data quality, individual participation, security, and accountability. For cybersecurity, the most relevant

of these are security, obviously, but also data minimization and accountability. If companies purge old data (or don't collect data they don't need), they will be less vulnerable to data theft. Similarly, if a statute includes robust accountability provisions that strongly punish companies for violations of the other principles, companies will have good reason to adopt procedures to avoid privacy and security violations. Moreover, legislation should require companies to have privacy and security procedures in place to ensure that those concepts are embedded in design and business model decisions from their inception, and that companies are forced to assess privacy and security risks in evaluating their business strategies.

Requiring companies to be transparent about their data collection and retention practices too would allow consumers to make informed decisions about which companies they feel comfortable sharing personal information.

4. What do you consider to be the greatest data security challenges today and in the future?

Advances in technology have enabled the dramatic growth of data collection, retention, and analytical capabilities. As a result, a broader and broader array of potentially less sophisticated entities are able to store sensitive personal information. Security is in many cases an afterthought at best. In the future, this trend is likely to continue — more companies collecting more data, keeping the data around for longer with a vague hope that it can be monetized. To the extent that leadership thinks about security at all, it is as a cost, not a profit center.

Currently, U.S. law imposes weak and unclear obligations on companies to disclose what personal information is collected by whom, and for what purpose. Consumers and advocates who wish to make privacy- and security-conscious decisions and recommendations are often completely unable to do so, as companies are not forced to disclose or describe their data practices.

5. What is the fastest and best way to get new innovations deployed to protect the safety, privacy, and security of consumers' financial data: government mandates that would pick technology winners and losers, or, allowing maximum competition for customers in the market by companies offering innovative security solutions and consumer protections against new, evolving, and changing threats that go beyond the requirements of a static law?

We do not believe that government should mandate specific technological approaches to data security. Rather, the law should put strong incentives on companies to adopt reasonable data security practices. Absent these incentives, market pressure alone might not result in adequate security practices, as consumers have little ability or competence to judge the data security practices of companies before entrusting them with their personal information.

Questions submitted by Ranking Member Maffei

1. Since 2001, the Federal Trade Commission (FTC) has used its regulatory authority to enter into 50 separate data security settlements with private companies that have failed to “provide reasonable protections for consumers’ personal information.” This has included cases against Twitter, Facebook, MySpace, and Google. In your opinion, is the FTC, other government agencies, or Congress doing enough to protect consumers’ privacy? And, if not, what recommendations do you have about what we should be doing?

The Federal Trade Commission has done an admirable job with the limited authority they have under Section 5 of the FTC Act. However, that law only provides for a broad prohibition on businesses committing unfair or deceptive trade practices. We were pleased to see the recent decision in the *FTC v. Wyndham Worldwide Corporation* supporting the FTC’s position that the prohibition on unfair practices requires companies to use reasonable security practices to safeguard consumer data. However, companies in other jurisdictions may still challenge the FTC’s ability to bring security cases under Section 5, and it remains unclear how aggressively the FTC may enforce privacy principles under that law. Historically, most FTC privacy cases relied upon a company violating an affirmative promise on how data would be treated. Companies had no obligation to make affirmative statements over how data would be used, to give consumers access to that data, or to give consumers choice around secondary usage of their information. The FTC has continued to be more aggressive on bad data privacy practices, but it is not at all clear how far their authority extends under Section 5, and currently it is very challenging for ordinary consumers to understand how their data is being collected and used. As such, consumers are not able to make informed choices about which services to use. Moreover, even to the extent that certain practices are prohibited by Section 5, the FTC in most cases does not have the ability to obtain statutory penalties for bad practices. As such, the vast majority of FTC settlements have no monetary component whatsoever, making them considerably less effective as a deterrent to bad privacy and security practices.

We have long advocated that Congress enact comprehensive privacy law to fill this gap. The United States remains one of two OECD nations (along with Turkey) not to have enacted privacy legislation. Such a law should, *inter alia*, allow the Federal Trade Commission to require notice and transparency about data security practices, give users meaningful control over how their information is collected and used, and require companies to use reasonable security procedures to safeguard the data that they store. This legislation should be backed up by vigorous enforcement mechanisms, including the ability of the Federal Trade Commission and state Attorneys General to obtain civil penalties

for violations, as well as a private right of action for aggrieved individuals to assert and protect their own rights.

2. The amount of personal information obtained **and** retained by private companies has exploded in the past few years. At the same time there have been an increasing number of data breaches that expose this data resulting in identity theft, credit card fraud, or other crimes. Do you believe that there are limits to what personal information private companies should collect about individuals and should there be any sort of policies regarding how they use this data and how long they are able to retain it?

We do not believe that there should be absolute limits on what sorts of data may be collected from individuals, or how long that data should be retained. Consumers should be empowered to make informed decisions about what data to share with whom, and privacy law should not paternalistically make those decisions for them. However, how data is collected from individuals should vary based on the sensitivity of the data and the context in which the data is obtained. Sensitive categories of information — including health, sexuality, and geolocation information — should typically be collected only with the informed consent of the individual. For some data collection and usage, it may be sufficient for companies to offer consumers an opportunity to affirmatively opt out if they decide to invoke their rights. And for certain data practices — such as the reasonable retention of data for fraud and security purposes — consumers cannot reasonably expect to exercise control over those data sets that pertain to them.

While we do not believe that legislated retention periods make sense for most data, companies should still adhere to basic data minimization principles: companies should only collect and retain data that is reasonably necessary for clearly articulated purposes. Obviously, companies will not be able to detail precisely every potential research or analytical use of each data element in advance, so we support the idea contained in the 2012 White House privacy report that uses that are *contextually related* to purposes communicated to or understood by a consumer should be permitted without getting new consent from the user. On the other hand, companies should not blithely keep all personal data on a vague hope that a monetization strategy will be developed one day. At the very least, transparency requires that companies disclose their data minimization and retention policies so that consumers, regulators, and advocates can assess their practices and make informed choices and recommendations.

3. In recent years IT devices able to monitor, track, and analyze consumer behavior have become smaller, faster, cheaper to acquire, and more powerful. What challenges do emerging technologies, including facial recognition and behavior profiling techniques, pose to personal privacy

and security in both cyberspace and physical space, such as a department store, for instance.

Technologically, we are reaching a point where all that we do — even inside our homes — could be recorded, stored, and analyzed by potentially dozens of entities (as well as the government). The key question is what sort of policy limitations we put in place to limit what data can be collected about us, or to give us control over that collection. Just because data *can* be collected about us does not mean that it *should* be. Human beings need zones where they can exist unobserved without the judgment of humanity weighing upon them. People need outlets where they can access or voice controversial or unpopular opinions, without worrying that their communications will go down on their permanent records.

In the physical world, CDT is very concerned about a future world where all our movements and behaviors can be tracked by entities with whom we have no relationship, either because of the signals being generated by our devices or because of increasingly sophisticated biometric identification technology. Some limited commercial data collection may be reasonable without affirmative consent — either for short-term in-store analytics or to compare with identifiers associated with fraudulent or illegal behavior. However, longer term profiles that retain information about an individual or device over different contexts — whether one location over different times, or entirely different places — should probably only be collected with the informed permission of the individual.

*Responses by Mr. Steven Chabinsky*

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY  
SUBCOMMITTEE ON OVERSIGHT  
AND  
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

**"Can Technology Protect Americans from International Cybercriminals?"**

**RESPONSE TO QUESTIONS FOR THE RECORD**

**STEVEN R. CHABINSKY**  
(in his personal capacity)

**Response to questions submitted by Chairman Broun and Chairman Bucshon**

- 1. What can we do to protect patient privacy and ensure that there is sufficient security to protect patient records in the healthcare and insurance industries?**

The risk of healthcare data breaches likely will continue to rise as (a) patient information increasingly is stored and transferred in electronic form, and (b) patient electronic records are shared beyond their point of origin to multiple parties and across multiple devices.

In order to better protect patient privacy, consideration first should be given to allowing patients greater control over whether and how sensitive health data should be stored and shared in light of the risks of improper disclosure versus the benefits of improved healthcare. Second, planning in advance for breaches should lead healthcare and insurance providers to implement greater technical, physical, and administrative controls for the most sensitive data, which likely will include end-to-end encryption, anonymization, pseudonymization, and at times the deletion of certain data elements altogether. Third, role-based audited access to specific portions of a patient's medical records (distinguishing the types and fields of data available to a specific doctor, nurse, pharmacist, etc.), as further controlled through the use of digital certificates, is another effective means to limit the improper disclosure of protected patient records. Finally, healthcare providers and the insurance industry must consider cybersecurity within an enterprise risk management program (to include consideration of the NIST cybersecurity framework or similar guidelines and standards), and should review the extensive resources made available by the U.S. Department of Health and Human Services (HHS) Office of the National Coordinator for Health Information Technology (ONC) at <http://www.healthit.gov/providers-professionals/ehr-privacy-security>.

- 2. Multiple law enforcement agencies have varying degrees of jurisdiction over cyber intrusions. Is there a sufficient level of communication and information sharing**

among them that allows for a coordination of resources and intelligence to help everyone do a better job of catching cybercriminals?

- a. Is there room for improvement in agency collaboration to minimize turf or jurisdictional wars?

Background on Jurisdiction. At the Federal level, and pursuant to statute [United States Code Title 18, Section 1030(d)], the United States Secret Service and the FBI generally share jurisdiction to investigate *criminal* computer intrusions. According to the same statute, that authority must be exercised in accordance with an agreement between the Attorney General and the Secretary of Homeland Security. In addition to the FBI and Secret Service, military criminal investigative organizations and a number of federal Inspectors General also have emphasized their role in investigating cybercrime. The Intelligence Community also plays a role in better understanding cybercrime, having the ability to gain information about foreign intrusion attempts before they hit our shores and a more sophisticated understanding of the potential interaction between nation-states and criminal organizations.

Background on Coordination of Resources and Intelligence. By Presidential mandate beginning with President Bush and extended by President Obama, the common coordinating point for cyber threat investigations is the National Cyber Investigative Joint Task Force. This collaborative structure is organizationally sound. As stated on the FBI's website, the NCIJTF serves as "the focal point for all government agencies to coordinate, integrate, and share information related to all domestic cyber threat investigations. The FBI is responsible for developing and supporting the joint task force, which includes 19 intelligence agencies and law enforcement, working side by side to identify key players and schemes. Its goal is to predict and prevent what's on the horizon and to pursue the enterprises behind cyber attacks."

Improving Current Levels of Coordination. A number of areas might be considered to improve coordination. First, in terms of resources, although government policies continue to emphasize multi-agency collaboration, I am unaware of any agencies being appropriated dedicated resources to assign their personnel to multi-agency environments. This leaves agencies having to take resources out of their own to fulfill these important roles. As a result, there is reason to consider within agency appropriations the specific funding of personnel that are detailed to other agencies (to include to the NCIJTF, as well as to DHS' US-CERT, DoD's Cyber Command, the White House's Cybersecurity Office, the ODNI, and other multi-agency environments), as well as to coordinate at the Field level with the FBI Cyber Crime Task Forces, and to support the public/private partnerships of InfraGard and the Secret Service Electronic Crimes Task Forces (and to ensure they are working together). Second, consideration might be given to determine if, under the FBI/Secret Service MOU or otherwise, federal law enforcement agencies follow the same investigative guidelines, as may be recommended to foster joint investigations and task force efforts. Third, with respect to

information sharing, it is likely that the FBI routinely disseminates far greater amounts of cyber intrusion information than it receives from other law enforcement agencies, based not only on the relative size of its cyber program but as well as a result of the mature processes it applies for producing and distributing standardized intelligence products (such as assessments, bulletins, and raw reports). In the absence of routine cyber reporting from law enforcement agencies other than the FBI, it becomes even more essential to foster NCIJTF and Task Force collaboration, to include the resources and policies necessary for detailees to check home agency databases and share any “hits” regarding another agency’s pending investigations.

**3. What can be done to help banks, payment companies and merchants better collaborate on industry standards and innovative solutions to data breaches and cybercrime for electronic financial transactions?**

Over time, there may be opportunities to determine whether NIST can play a greater role in testing current and emerging payment technologies. Still, I am already encouraged by industry’s recognition of the need to collaborate on these issues, as evidenced in part by the creation this past February of a merchant and financial trade association cybersecurity partnership to increase information sharing and to explore better card security technology. In this regard, I am particularly impressed by the efforts of the Retail Industry Leaders Association (RILA) and its formation of a Retail Cybersecurity Leaders Council, which I addressed last month. With respect to the broader partnership, RILA is teaming with the Financial Services Roundtable (FSR), joined by the American Bankers Association (ABA), the American Hotel & Lodging Association (AH&LA), The Clearing House (TCH), the Consumer Bankers Association (CBA), the Food Marketing Institute (FMI), Independent Community Bankers of America (ICBA), the International Council of Shopping Centers (ICSC), the National Associations of Convenience Stores (NACS), the National Grocers Association (NGA), the National Restaurant Association (NRA), and the National Retail Federation (NRF). In addition to these efforts, RILA is partnering with the non-profit National Cyber-Forensics and Training Alliance (NCFTA), which itself partners with law enforcement (including the FBI), to share cyber threat information.

**4. What do you consider to be the greatest data security challenges today and in the future?**

The greatest data security challenge today and for the foreseeable future very well may involve educating society about risk. We continue to expand the types and volume of sensitive data we store electronically, and we increasingly rely upon converged networks to control our critical infrastructure, all without understanding, quantifying, and accepting the residual risk. Instead, despite a steady stream of warnings, we seem surprised and even angered when intrusions continue to occur with increasing frequency and impact. It is worth considering whether certain data and certain systems

should not be remotely accessible by anyone seeking to harm us, acting without fear of getting caught, using ubiquitous technologies, from anywhere in the world. With a proper understanding of risk, we are more likely to identify, scope, and resolve issues relating to data segregation, systems isolation, privacy requirements, security demands, and sustainable models for achieving threat deterrence.

5. **How easy is it for someone to buy malware to commit a similar crime to the recent Target breach?**
  - a. **How technically savvy would that person have to be in order to utilize the malware successfully?**
  - b. **Is malware becoming a virtual commodity product?**

Over the past decade, malware increasingly is created and modified by the few, and purchased for use by the many. “Coders,” the term used for people who actually are writing the lines of malicious software code, focus on staying up-to-date on advancements in software, hardware, and applications so that their “custom” exploits can target unknown or unpatched vulnerabilities. Still, coders also create and modify customizable malware toolkits with easy to use interfaces requiring no user sophistication. These kits have multiple exploits that attempt to target a system one-at-a-time. If one particular exploit doesn’t work, the next is tried. As soon as one does work, the designated executable is downloaded and run on the system. These kits appeal to those in the cyber world who cannot write their own malware, or who do not have the time or patience to test individual exploits manually. An additional benefit to the criminal is that these kits are easily updated and expanded, allowing hackers to add capabilities for a specific crime. The term “commodity malware” is widely in use today, referencing the vast availability of these crimeware toolkits for easy purchase.

Most every cyber criminal is a member of at least one online forum, website, or chat service. Some of these are completely public, while others have more requirements for entry, such as vetting by current members or through tests of skill. Most of these sites have discussion areas for trading tips and techniques, market areas for buying and selling crimeware toolkits, and means to report and evaluate fellow users, just like the rating system on eBay. As a result, although it may be difficult for a criminal to commit the exact same crime as those recently brandishing the headlines (and which, therefore, also galvanized the security community to tighten certain defenses), we can expect similar breaches that result in large data compromises and which will often present themselves to criminals as a result of third party vendor weaknesses.

6. **From your experience in the FBI, and from what you have heard in the community, what can you tell us about how other countries, such as Russia, facilitate and incentivize the operations of international crime syndicates? Do these countries benefit from hackers’ exploits?**

International cybercrime syndicates are more likely to thrive within countries having a history of organized crime groups that are protected either because of government corruption or actual government alliances. In such settings, cybercriminals appear to operate with a certain level of impunity. Indeed, even where Russia has prosecuted major cybercriminals, the results tend not to result in jail time, leaving many to wonder whether undisclosed deals were made. Public reports also suggest that Russian Intelligence has taken advantage of homegrown cybercriminals to launch attacks against neighboring Estonia and Georgia, both as a means of extending its nation-state capabilities and in order to retain a level of deniability. In addition, criminal tools often find their way into the hands of government actors, at times without the malware seller knowing the true identity of the buyer.

7. **Does the technological capability exist today to take offensive countermeasures in response to a cyber-attack? If so, what are they specifically, and should the U.S. government as well as businesses be allowed to employ them as a defensive measure?**

Capabilities exist and can be further developed across a wide range of response options that would allow the government and industry to better detect and attribute criminal activities, as well as to mitigate or altogether eliminate the harm caused by criminal acts. Some of these opportunities do not require technology at all, but merely the ability to sign in to a bad guy's computer (where the victim's files are stored) using the same name and password that the bad guys routinely code into the malware they unlawfully place on victim computers. Consider the March 13, 2014 report from Bloomberg Businessweek indicating that, from a capabilities perspective, one recent high profile corporate victim easily could have located on the bad guy's computer the tens of millions of records that had been stolen from it and simply deleted or encrypted all of it. Instead, the loss remains the subject of an international criminal investigation, class action lawsuits, calls for billions of dollars in new technology deployments (the costs of which will be borne by consumers and shareholders), and continuing Congressional hearings:

*"The malware had user names and passwords for the thieves' staging servers embedded in the code, according to Jaime Blasco, a researcher for the security firm AlienVault Labs. [The victim's] security could have signed in to the servers themselves—located in Ashburn, Va., Provo, Utah, and Los Angeles—and seen the stolen data sitting there waiting for the hackers' daily pickup."*

Meanwhile, in Luxembourg, a company called itrust consulting (which is a private Computer Security Incident Response Team) published a report exposing suspected Chinese economic espionage infrastructure, methodologies, and tools. The company acquired extensive access to the hacker infrastructure by creating an exploit to remotely

take control of the bad guy's command & control servers. The write up is available online at [http://www.malware.lu/Pro/RAP002\\_APT1\\_Technical\\_backstage.1.0.pdf](http://www.malware.lu/Pro/RAP002_APT1_Technical_backstage.1.0.pdf).

In another case, the Computer Emergency Response Team of the Republic of Georgia identified a hacker by turning the tables on him. In short, CERT-Georgia took the hacker's own malware, placed it in a document they believed the hacker would steal, which the hacker in fact did steal. Once stolen, the good guys used the hacker's own malware to infect his computer, to physically locate him, video tape him at his computer, search his computer, and link him to his cohorts in Germany and Russia. The public write-up of those countermeasures, complete with pictures, is available here: [http://dea.gov.ge/uploads/CERT\\_DOCS/Cyber Espionage.pdf](http://dea.gov.ge/uploads/CERT_DOCS/Cyber_Espionage.pdf)

**8. How often do cybercriminals get caught and face punishment after they perform a crime?**

Unfortunately, there is little by way of published data to make this determination. Certainly, there is a perception that only a small percentage of cybercriminals get caught and punished. Still, news reports do evidence continued successes in combatting global cybercrime, and the Department of Justice maintains a website at <http://www.cybercrime.gov> that provides information about many successes in the form of Press Releases.

To gain a better view of success in this area, one could envision the FBI's Uniform Crime Reporting Program being used specifically to track computer intrusions. That program includes the concept of "clearances," under which law enforcement agencies can indicate when cases are resolved by arrest, charges being filed, and the matter being turned over for prosecution.

In the meantime, potential federal data sources that could be used to compare known incidents with open cases and federal prosecutorial disposition (meaning the number of investigative matters received by US Attorneys Offices, the number of defendants charged, cases charged, and defendants sentenced) include: (a) FISMA reporting indicating criminal activities discovered on federal agency systems and whether they have been referred to, and opened as cases by, federal law enforcement; (b) FBI and Secret Service case openings; (c) computer intrusion matters reported through the Internet Crime Complaint Center and referred to both federal and state/local law enforcement; (d) data breaches reported to or otherwise known by the Federal Trade Commission and the Department of Health and Human Services; (e) computer intrusions known to the Securities Exchange Commission through public filings; and, (f) computer intrusions reported by the Banking and Finance Sector within Suspicious Activities Reports.

**Response to questions submitted by Rep. David Schweikert**

- 1. Do you believe that the NIST framework will be adopted due to the perceived benchmark for courts to evaluate the effectiveness of a company's cybersecurity program in the context of data breach litigation?**

It is likely that the NIST Framework will receive heightened attention, if not outright adoption, by companies partially out of concern that the Framework will be considered by lawyers and courts as a benchmark for assessing industry best practices. However, to the extent the Framework raises its head in litigation, defense counsel will be quick to note that a company can make intelligent risk management choices using NIST's guidance that still result in data breaches. Ultimately, the Framework is more about walking companies through the right set of questions, rather than standardizing a right set of answers or defining a common measure of success. From a litigation perspective, therefore, the NIST Framework might stand for the proposition that officers, directors and business owners would do well to engage actively and continuously in a detailed evaluative process of their cyber risk, regardless of the business judgments they make in response.

- 2. Americans have been behind the eight ball in cybersecurity for some time now. However, as we pay more attention to this issue and provide more resources to shore up our defenses, has the nature of the threat changed?**

In response to our shored up defenses, the nature of the threat continues to escalate and/or shift to other vectors of intrusion. Unfortunately, despite billions of dollars in effort, the problem continues to get worse with no signs of leveling off no less declining. This negative trend will continue in my opinion until we learn to focus more of our technologies, policies, and resources on deterring the threat actors rather than seeking to make potential victims invulnerable. Hackers have ready access to inexpensive commodity malware and customized exploits and can, as required, take advantage of a range of vectors including remote intrusions, supply chain attacks, and insider access. While much is said about the fact that many companies and agencies do not currently practice good cyber hygiene (which certainly is true), there is no data to suggest that spending billions of dollars more to achieve that level of diligence would do anything to prevent persistent, sophisticated intrusions of the kind we routinely observe and with which we are most concerned as a nation. Therefore, I agree that we are behind the eight ball, with our efforts blocked at every turn. Let us refocus then, and consider new approaches to detect, identify, and respond to those who keep hitting us hard with the pool cue.